BITDEFENDER SECURITY FOR SHAREPOINT

Administratorhandbuch

bitdefender®

BitDefender Security for SharePoint 3.5
Administratorhandbuch

Veröffentlicht 2011.05.06

Copyright© 2011 BitDefender

Rechtlicher Hinweis

Alle Rechte vorbehalten. Bestandteile dieses Handbuches dürfen weder in elektronischer noch mechanischer Form reproduziert werden. Dies gilt auch für das Fotokopieren, Aufnehmen oder jegliche andere Form von Datenspeicherung oder Informationsbeschaffung, ohne die Zustimmung von BitDefender. Ausnahmen gelten für Zitate in Verbindung mit Testberichten. Der Inhalt darf in keiner Weise verändert werden.

Warnung und Haftungsausschluss. Dieses Produkt bzw. Dokument ist urheberrechtlich geschützt. Die inhaltlichen Informationen in diesem Dokument sind „faktenbasiert" und enthalten keinen Garantieanspruch. Obwohl dieses Dokument mit äußerster Sorgfalt erstellt und geprüft wurde, übernehmen die Autoren keinerlei Haftung für eventuell auftretende Schäden bzw. Datenverlust die direkt oder indirekt unter Verwendung dieses Dokumentes entstehen könnten oder bereits entstanden sind.

Dieses Handbuch enthält Verweise auf andere, nicht von BitDefender erstellte Webseiten, die auch nicht von BitDefender kontrolliert werden. Somit übernimmt BitDefender auch keine Verantwortung für den Inhalt dieser Webseiten. Der Besuch dieser Webseiten erfolgt somit auf eigene Gefahr. BitDefender stellt diese Verweise aus Gründen der Anwenderfreundlichkeit zur Verfügung, was nicht bedeutet, dass BitDefender in jeglicher Art und Weise Verantwortung oder Haftung für diese Webseiten und deren Inhalt übernimmt.

Warenzeichen. Es erscheinen eingetragene Warenzeichen in diesem Dokument. Alle eingetragenen und nicht eingetragenen Warenzeichen in diesem Dokument sind das alleinige Eigentum der jeweiligen Besitzer.

bitdefender

Inhaltsverzeichnis

Vorwort ..... **vii**
1. Verwendete Konventionen vii
1.1. Typografie vii
1.2. Symbole viii
2. Struktur viii
3. Ihre Mithilfe ix

Beschreibung ***1***

1. Funktionen und Vorteile **2**

Installation ***4***

2. Vor der Installation **5**
2.1. Systemanforderungen 5

3. BitDefender Security für SharePoint installieren **6**
3.1. Neue Installation 6
3.1.1. Schritt 1/8 - Willkommen 7
3.1.2. Schritt 2/8 - Endbenutzer-Lizenzvereinbarung 7
3.1.3. Schritt 3/8 - Prüfung vor der Installation 8
3.1.4. Schritt 4/8 - Zu installierende Produkte auswählen 9
3.1.5. Schritt 5/8 - Produkt-Update-Optionen konfigurieren 10
3.1.6. Schritt 6/8 - Vorfallsberichte konfigurieren 11
3.1.7. Schritt 7/8 - Installation starten 12
3.1.8. Schritt 8/8 - Installation abgeschlossen 13
3.2. Bestehende Installation ändern 13
3.3. Upgrade für eine ältere Version installieren 13

4. BitDefender ändern, reparieren oder entfernen **15**
4.1. Modifiziere BitDefender 15
4.2. BitDefender reparieren 16
4.3. BitDefender deinstallieren 16

Konfiguration und Verwaltung ***17***

5. Erste Schritte **18**

6. Dashboard **20**
6.1. Statusbereich 20
6.1.1. Serverprüfung 21
6.1.2. Update Status 22
6.1.3. Lizenzstatus 23
6.2. Produkt-Status 25

7. Überwachung **26**
7.1. Statistik 27
7.1.1. Statistiken säubern 28
7.2. Berichte 28
7.2.1. Berichte verwalten 30
7.2.2. Berichte erstellen 30

7.2.3. Berichte löschen 33
7.3. Benachrichtigungen & Protokolle 34
7.3.1. Protokolle 34
7.3.2. Benachrichtigungen 36
7.3.3. Benachrichtigungseinstellungen 40
7.4. Quarantäne 43
7.4.1. Die Quarantäne verwalten 43
7.4.2. Quarantäne löschen 44
7.5. Geplante Aufgaben 45
7.5.1. Geplante Aufgaben verwalten 45
7.5.2. On-Demand Prüfaufgaben 46
7.5.3. Update-Aufgaben 52
7.5.4. Aufgaben zur Berichterstellung 56

8. Serverprüfung 64
8.1. Echtzeitprüfung 64
8.1.1. Konfiguriere Microsoft SharePoint AntiVirus Einstellungen 65
8.1.2. Prüfungsprofile 66
8.2. Prüfvorgang 73
8.2.1. Dateien und Ordner prüfen 74
8.2.2. Prüfungsprofile 75
8.3. AntiViren-Schutz Prüfung 82

9. Aktualisierung 84
9.1. Aktualisierung 85
9.1.1. Update-Informationen 85
9.1.2. Produkt-Update 85
9.2. Update-Einstellungen 87
9.2.1. Update-Planung konfigurieren 87
9.2.2. Konfiguriere Produkt Updates 88
9.3. Update Locations 90
9.4. Update Benachrichtigungen 91
9.5. Update zurückrollen 92

10. Allgemein 93
10.1. Virenbericht 93
10.2. Vorfallsberichte 94
10.3. importieren/exportieren der Management Konsole Einstellungen 95
10.3.1. Policy-Einstellungen exportieren 95
10.3.2. Policy-Einstellungen importieren 95

11. Lizenz 96
11.1. Kaufe die Vollversion des Produktes 96
11.2. Produkt registrieren 96
11.3. Ein BitDefender Benutzerkonto registrieren 97

12. Hilfe 99

Fehlerdiagnose und Problemlösung 100

13. BitDefender Konfigurationsreparatur Tool 101

14. Support 103
14.1. BitDefender-Support-Center 103
14.1.1. BitDefender Knowledge Base 103

14.1.2. BitDefender Support-Forum 104
14.1.3. Video Tutorials 104
14.1.4. Produktdokumentation 104
14.2. Hilfe anfordern 104
14.3. BitDefender Support Tool 105
15. Kontaktinformation 108
15.1. Kontaktadressen 108
15.2. Händler vor Ort 108
15.3. BitDefender Geschäftsstellen 108
15.3.1. Deutschland 109
15.3.2. Rumänien 109
15.3.3. USA 109
15.3.4. Großbritannien und Irland 109
15.3.5. Spain 110
Glossar 111

Vorwort

Dieses Benutzerhandbuch ist für alle Unternehmen vorgesehen, die sich für **BitDefender für SharePoint Server** als Sicherheitslösung für ihre SahrePoint Server entschieden haben. Die in diesem Dokument beschriebenen Informationen sind nicht nur für IT-Profis gedacht, sondern auch für all diejenigen die unter Windows arbeiten können.

Dieses Handbuch beschreibt **BitDefender für SharePoint Server** die Firma und das Team die es konzipiert haben, es wird Sie durch den Installationsprozess führen und Ihnen zeigen wie Sie das Produkt konfigurieren können. So lernen Sie wie Sie **BitDefender Security für SharePoint Server** verwenden, aktualisieren, testen und anpassen können. So erfahren Sie wie Sie BitDefender am Effektivsten einsetzen können.

Viel Spaß mit diesen nützlichen und informativen Handbuch.

1. Verwendete Konventionen

1.1. Typografie

Um die Lesbarkeit zu fördern werden verschiedene Arten von Textstilen verwendet. Die jeweiligen Bedeutungen entnehmen Sie bitte der Tabelle unterhalb.

Erscheinungsbild	Beschreibung
`sample syntax`	Syntaxbeispiele werden in einer Schriftart mit `fester Laufweite` angegeben.
http://www.bitdefender.com	Verweise (Links) auf externe Inhalte wie z.B. Web-Seiten oder FTP-Server.
sales@bitdefender.com	Verweise auf E-Mail-Adressen, z.B. zur Kontaktaufnahme.
„Vorwort“ (S. vii)	Interne Verweise (Links) auf beliebige Stellen innerhalb dieses Dokuments.
`filename`	Dateien und Verzeichnisse werden in einer Schriftart mit `fester Laufweite` angegeben.
option	Optionen wie z.B. Schaltflächen oder Checkbox-Elemente werden in **fett gedruckt** angegeben.
`sample code listing`	Beispielquelltexte werden in einer Schriftart mit `fester Laufweite` angegeben.

1.2. Symbole

Bei diesen Symbolen handelt es sich um Hinweise innerhalb des Textflusses welche mit einer kleinen Grafik markiert sind. Hierbei handelt es sich um Informationen die Sie in jedem Fall beachten sollten.

Beachten Sie
Diese Bemerkung dient lediglich zur Überprüfung. Notizen enthalten nützliche Informationen wie zum Beispiel einen Verweis auf ein verwandtes Thema.

Wichtig
Diese Art von Hinweis sollte in jedem Fall gelesen werden. Es werden signifikante Informationen zum jeweiligen Thema bereitgestellt. Es wird nicht empfohlen diese zu übergehen.

Warnung
Diese kritische Information sollten Sie mit höchster Aufmerksamkeit verfolgen. Hier angegebenen Anweisungen und Informationen sollten Sie auf jeden Fall Beachtung schenken. Sie sollten diese Informationen sorgsam lesen und verstanden haben, da es sich um eine höchst prekäre Thematik handelt.

2. Struktur

Dieses Handbuch ist in vier Abschnitte unterteilt, welche die folgenden Hauptthemen beinhalten: Beschreibung, Installation, Konfiguration und Verwaltung, Fehlerdiagnose und Problemlösung. Ausserdem ist ein Glossar enthalten welcher einige technische Begriffe erklärt.

Beschreibung. BitDefender Security für SharePoingt Server und dessen Funktionen werden vorgestellt.

Installation. Schritt-für-Schritt Anleitung zur Installation von BitDefender an einem Arbeitsplatz. Hierbei erhalten Sie ausführliche Informationen für eine erfolgreiche Installation von **BitDefender für SharePoint Server**. Beginnend mit den Installationsvoraussetzungen werden Sie durch den gesamten Installationsprozess begleitet. Zusätzlich wird beschreiben wie eine Deinstallation von BitDefender durchzuführen ist.

Konfiguration und Verwaltung. Beschreibung der Grundkonfiguration und Wartung von BitDefender. Diese Abschnitte erklären alle Optionen von **BitDefender Security für SharePoint Server**, wie das Produkt zu registrieren ist, wie ein Prüfvorgang für den SharePoint Server und wie ein Update von BitDefender durchgeführt werden kann.

Fehlerdiagnose und Problemlösung. Beschreibt wie Sie Hilfe bzw. Unterstützung zu dem Produkt erhalten und erhält zusätzlich eine Liste mit den am häufigsten gestellten Fragen (FAQ).

Glossar. Im Glossar werden technische Ausdrücke und seltene Bezeichnungen erklärt, die in diesem Dokument zu finden sind.

3. Ihre Mithilfe

Wir laden Sie dazu ein uns bei der Verbesserung dieses Dokuments mitzuhelfen. Wir haben sämtliche Informationen in diesem Dokument bestmöglich überprüft um somit die Qualität sicherzustellen.

Falls Sie dennoch Fehler finden, so teilen Sie uns diese bitte mit indem Sie uns per E-Mail unter der Adresse documentation@bitdefender.com kontaktieren.

Wichtig
Bitte verfassen Sie bitte alle auf die Dokumentation bezogenen E-Mails auf Englisch.

Beschreibung

1. Funktionen und Vorteile

BitDefender Security für SharePoint führt On-Access, Echt-Zeit Scans von hoch- und heruntergeladenen Dateien in Dokumenten Bibliotheken und Listen durch, mit exzellenten Säuberungsraten und eine Option infizierte Dokumente in die Quarantäne zu verschieben.

Sobald eine Datei hoch- oder heruntergeladen wird, wird sie sofort geprüft. Falls BitDefender AntiVirus Scanner eine infizierte Datei findet, wird die Datei entsprechend der vom Administrator gewählten Regel behandelt wird. Zusätzlich kann BitDefender eingestellt werden, dass die Administratoren über laufende Vorgänge per E-Mail und/oder NetSend benachrichtigt werden.

On-Demnad Prüfungseinstellungen erlauben geplante System-Prüfungen ausserhalb der spitzen Arbeitszeiten, ohne die Gesamtleistung oder Verfügbarkeit des Systems zu beeinträchtigen.

Die fortschrittlichen Berichts- und Erfassungswerkzeuge und Integration mit dem BitDefender Management Server werten BitDefender Security für SharePoint auf, als eine Sicherheitslösung für Ihre Kollborationsanforderungen.

Hauptmerkmale

- Nahtlose Integration mit dem SharePoint Server um den Prüfvorgang zu optimieren und zu verschnellern
- Proaktiver und heuristischer Schutz vor Zero-Day Threats
- Voreingestellte Antivirus Prüfungsprofile erlauben mehr Flexibilität
- Zertifizierte Antivirus Engines
- Zentralisierte Management-Unterstützung durch Intergration mit BitDefender Server

BitDefender Technologien

B-HAVE. BitDefender Security für SharePoint beinhaltet B-HAVE, eine patentierte Technologie, die das Verhalten potentiell gefährlicher Codes innerhalb einer virtuellen Umgebung analysiert, wobei False Positives beseitigt werden und die Erkennungsrate für neue und unbekannte Malware erheblich gesteigert wird.

Zertifizierte Antivirus Engines. Die Scan Engines von BitDefender wurden mit ihrer B-HAVE Technologie bereits mehrfach von ICSA Labs, Virus Bulletin und Checkmark für den besten vorbeugenden Virenschutz, der zurzeit erhältlich ist, ausgezeichnet.

Dienste

- Fortgeschrittenes Update-System

Für einen dauerhaften Schutz, erhält die Lösung ständig die neusten Updates und Patches, wobei Sie den Zeitpunkt der Aktualisierung wählen können: On-Demand, zeitlich konfiguriert oder automatisch.

- Upgrades

  Registrierte Nutzer profitieren von kostenfreien Upgrades auf jede neue Version des für sie lizenzierten Produktes während der gesamten Lizenzlaufzeit. Für ehemalige Kunden stehen ebenfalls spezielle Angebote zur Verfügung.

- Kostenloser Technischer 24-Stunden Support

  Geprüfte Mitarbeiter stehen BitDefender Business Kunden mit einem kostenlosen 24-Stunden Support zur Verfügung, sowohl Online, als auch per Telefon oder E-Mail. Zusätzlich steht eine Online-Datenbank zur Verfügung, mit Antworten zu häufig gestellten Fragen, und oft behandelten Themen.

Installation

2. Vor der Installation

Zur Vorbereitung der Installation müssen Sie die folgenden Schritte ausführen:

- Stellen Sie sicher, dass der Computer die Systemanforderungen erfüllt.
- Melden Sie sich als Administrator am Computer an.
- Entfernen Sie ähnliche Sicherheits-Software vom Computer. Die gleichzeitige Nutzung mehreren Sicherheitsprogrammen kann die jeweilige Funktion stören und massive Probleme auf Ihrem Computer verursachen.

Beachten Sie
BitDefender Security for SharePoint unterstützt keine SharePoint-Server in einer Farm-Umgebung.

2.1. Systemanforderungen

- **Betriebsystem:**
  - Microsoft Windows Server 2003 mit SP1 (SP2 wird empfohlen)
  - Microsoft Windows Server 2008 / Microsoft Windows Server 2008 R2
- Microsoft Office SharePoint Server 2007
- Microsoft Windows SharePoint Dienste 3.0
- Microsoft Internet Explorer Version 6.0 oder höher (level 1) oder Mozilla Firefox Version 3.0 oder höher (level 2)
- Minimum 1 GB freier Speicherplatz auf der HDD

3. BitDefender Security für SharePoint installieren

Zur Installation von BitDefender Security for SharePoint benötigen Sie die Installationsdatei. Es stehen 32-Bit- und 64-Bit-Varianten zur Verfügung. Verwenden Sie die Variante, die Ihrer Systemarchitektur entspricht.

Sie können die Installationsdatei entweder auf einer Installations-DVD bekommen oder aus dem Internet, z. B. von der BitDefender-Website herunterladen. Wenn Sie das Programm von einer DVD installieren, legen Sie die DVD in ein optisches Laufwerk und verwenden Sie die grafische Oberfläche, um auf den Inhalt der DVD zuzugreifen.

Das Installationspaket beinhaltet, ausser BitDefender Security für SharePoint Server, auch noch andere BitDefender Security für Windows Servers Produkte. Sie sollten alle Produkte, die Sie benutzen wollen, zur gleichen Zeit installieren. Installieren Sie nur BitDefender Security für SharePoint, werden Sie bei der späteren Installation anderer BitDefender Produkte, die existierende Installation modifizieren müssen. Als resultat dieser Aktion, kann es nötig sein einige Datein zu ersetzen. Dies kann dazu führen, dass temporär einige installierte Produkte nicht richtig funktionieren.

Je nachdem, ob Sie bereits Produkte aus dem Paket auf Ihrem Computer installiert haben, gibt es zwei Wege BitDefender Security for SharePoint zu installieren:

- Neue Installation - kein anderes Produkt des Installationspakets ist auf dem Computer installiert.
- Bestehende Installation ändern - mindestens ein anderes Produkt des Installationspaketes ist auf dem Computer installiert.

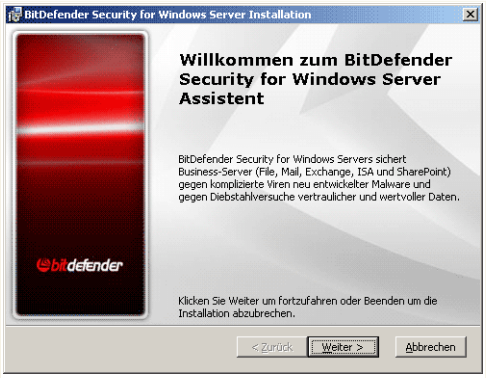
3.1. Neue Installation

Um eine frische Installation zu starten, finden Sie die Setup Datei und doppel-klicken sie: Ein Assistent wird erscheinen. Folgen Sie den Schritten, um die installation abzuschliessen.

Bevor die Installation beginnt, prüft BitDefender, ob eine neuere Version des Installationspaketes verfügbar ist. Sollte dies der Fall sein, so werden Sie gefragt, ob Sie dieses herunterladen möchten. Klicken Sie **Ja** um die neue Version herunterzuladen oder **Nein** um die Installation mit der bereits vorhandenen Datei fortzuführen.

Folgen Sie diesen Schritten, um BitDefender Security für SharePoint zu installieren:

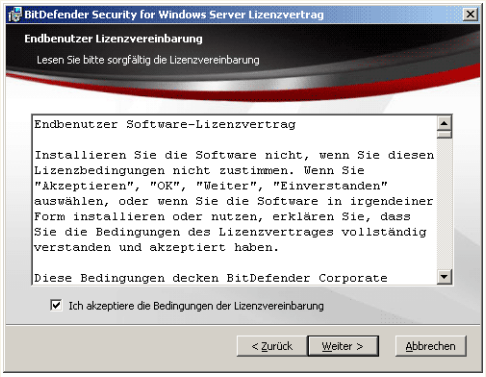
3.1.1. Schritt 1/8 - Willkommen


BitDefender Security for Windows Server Installation
Willkommen zum BitDefender Security for Windows Server Assistent
BitDefender Security for Windows Servers sichert Business-Server (File, Mail, Exchange, ISA und SharePoint) gegen komplizierte Viren neu entwickelter Malware und gegen Diebstahlversuche vertraulicher und wertvoller Daten.
bitdefender
Klicken Sie Weiter um fortzufahren oder Beenden um die Installation abzubrechen.
< Zurück
Weiter >
Abbrechen

Willkommen

Klicken Sie auf **Weiter**, um fortzufahren, oder klicken Sie auf **Abbrechen**, um die Installation abzubrechen.

3.1.2. Schritt 2/8 - Endbenutzer-Lizenzvereinbarung


BitDefender Security for Windows Server Lizenzvertrag
Endbenutzer Lizenzvereinbarung
Lesen Sie bitte sorgfältig die Lizenzvereinbarung
Endbenutzer Software-Lizenzvertrag
Installieren Sie die Software nicht, wenn Sie diesen Lizenzbedingungen nicht zustimmen. Wenn Sie "Akzeptieren", "OK", "Weiter", "Einverstanden" auswählen, oder wenn Sie die Software in irgendeiner Form installieren oder nutzen, erklären Sie, dass Sie die Bedingungen des Lizenzvertrages vollständig verstanden und akzeptiert haben.
Diese Bedingungen decken BitDefender Corporate
Ich akzeptiere die Bedingungen der Lizenzvereinbarung
< Zurück
Weiter >
Abbrechen

Endbenutzer-Lizenzvereinbarung

Bitte lesen Sie die Lizenzvereinbarung und wählen Sie **Ich akzeptiere die Bedingungen der Lizenzvereinbarung** und klicken Sie auf **Weiter**.

Beachten Sie
Wenn Sie diesen Bedingungen nicht zustimmen, klicken Sie auf **Abbrechen**. Die Installation wird abgebrochen und Sie werden das Setup verlassen.

3.1.3. Schritt 3/8 - Prüfung vor der Installation

BitDefender Security for Windows Servers Installation
Prüfung vor der Installation
Der Assistent ist bereit, Ihren Server vor der Installation zu prüfen.
Wenn Ihr Server mit Schad-Software infiziert ist, kann diese die Installation des BitDefender-Produkts verhindern oder beeinträchtigen. Klicken Sie auf "Prüfung starten", um den Server vor der Installation auf Anzeichen von Schad-Software zu überprüfen. Die Prüfung wird einige Minuten dauern. Haben Sie bitte etwas Geduld. Klicken Sie auf "Prüfung überspringen", wenn Sie diese Prüfung nicht durchführen und direkt mit der Installation fortfahren möchten.
Prüfung starten
Prüfung überspringen
< Zurück
Weiter >
Abbrechen

Prüfung vor der Installation

BitDefender kann vor der Installation kritische Bereiche Ihres Systems prüfen, um sicherzustellen, dass der Server frei von Infektionen ist.

Die Prüfung kann einige Minuten dauern. Klicken Sie auf **Jetzt prüfen**, um die Prüfung zu starten, oder klicken Sie auf **Prüfung überspringen**, um die Installation ohne Prüfung fortzusetzen.

Wichtig

Es wird dringend empfohlen, die Prüfung durchzuführen. Aktive Malware könnte die Installation stören oder sogar dazu führen, dass die Installation fehlschlägt. Falls eine Bedrohung entdeckt werden sollte, kann ein Neustart nötig sein, um sie zu entfernen.

3.1.4. Schritt 4/8 - Zu installierende Produkte auswählen

BitDefender Security for Windows Servers Installation
Kundenspezifische Einstellung
Wählen Sie die Art aus, wie die Eigenschaften installiert werden.
BitDefender Security for Windows Server
BitDefender Security for File Servers
BitDefender Security for Exchange
BitDefender Security for Mail Servers
BitDefender Security for SharePoint
Diese Komponente erfordert 27MB auf Ihrer Festplatte. Für die Unterkomponenten sind 0KB auf Ihrer Festplatte nötig.
Alle Produkte in diesem Paket sind Vollversionen und können für 30 Tage getestet werden. Wenn Sie sie kaufen möchten, kontaktieren Sie bitte Ihren BitDefender-Händler.
Installationsort: C:\Program Files\BitDefender\
Durchsuchen
Zurücksetzen
Disk Verwendung
< Zurück
Weiter >
Abbrechen

Zu installierende Produkte auswählen

Wählen Sie BitDefender Security for SharePoint, klicken Sie auf den entsprechenden **Pfeil** und klicken Sie dann auf **Wird auf lokaler Festplatte installiert** in dem Shortcut-Menu.

Der Standard Installationsordner wird in der unteren Hälfte des Fensters angezeigt. Um einen anderen Ordner zu wählen, klicken Sie **Browse**, wählen Sie den Ordner und klicken Sie dann **OK**, um den Ort festzulegen.

Beachten Sie

Sie können auch andere BitDefender-Produkte für Windows-Server installieren. Wählen Sie sie wie oben beschrieben aus. Je nach gewähltem Produkt können einige zusätzliche Schritte im hier beschriebenen Installationsprozess auftauchen.

Klicken Sie auf **Weiter**.

3.1.5. Schritt 5/8 - Produkt-Update-Optionen konfigurieren

BitDefender Security for Windows Servers Installation
Aktualisierungsoptionen
Wählen Sie für jede Aktualisierungsart der entsprechenden Optionen.
Erfordert kein Anhalten/Starten des Server Traffic oder Neustart des Servers
Ich möchte den Installationszeitpunkt bestimmen
täglich
an
1:00 AM
Erfordert einen Start/Stop des Server Traffic, aber keinen Neustart des Server.
Ich möchte den Installationszeitpunkt bestimmen
täglich
an
1:00 AM
Bedingt den Neustart des Servers
Ich möchte den Installationszeitpunkt bestimmen
täglich
an
1:00 AM
Keine automatischen Aktualisierungen, auch nicht, wenn dies bedeutet, dass mein Server weniger gut gesichert ist.
< Zurück
Weiter >
Abbrechen

Produktaktualisierungsoptionen

Produkt Updates regelmäßig zu installieren, ist für die Sicherheit Ihres Servers sehr wichtig. Abhängig von dem Grad der Beeinträchtigung des Servers, gibt es drei Arten von Produkt Updates:

- Produkt Updates, die kein anhalten des Server Verkehrs oder Neustart des Servers verlangen
- Produkt Updates, die ein Anhalten des Server Verkehrs verlangen, aber keinen Neustart des Servers
- Produkt Updates, die einen Neustart des Server verlangen

Um automatische Downloads und Installation für jede Art von Produkt Updates zu konfigurieren, wählen Sie eine der folgenden Optionen:

Automatisch installieren
Wählen Sie diese Option und BitDefender wird automatisch Produkt Updates laden und installieren. Dies ist die empfohlene Wahl für Produkt Updates, die kein Anhalten des Server Verkehrs oder Neustart des Servers verlangen.

Zu einer von mir bestimmten Zeit installieren
Wählen Sie diese Option, wenn sie wollen, dass BitDefender verfügbare Updates zu einer gewissen Zeit installiert. Wählen Sie aus der Liste das Datum (Tag und Zeit) wann dies geschehen soll.

Auf diese Weise können Sie BitDefender konfigurieren Produkt Updates an Zeiten durchzuführen, zu denen die wenigsten Störungen der Server Aktivität zu erwarten sind (nachts bspw.)

Ich möchte den Installationszeitpunkt bestimmen
Wählen Sie diese Option, wenn Sie wollen, dass BitDefender automatisch Produkt Updates lädt, sie aber entscheiden, wann sie installiert werden sollen. Dies ist

die empfohlene Auswal für Produkt Updates, die ein Anhalten des Server Verkehrs und einen Neustart des Servers verlangen.

Um die automatische Produktaktualisierung zu deaktivieren, markieren Sie das Kästchen **Keine automatischen Produktaktualisierungen, auch nicht wenn dadurch mein Server weniger gut gesichert ist**.

Klicken Sie auf **Weiter**.

3.1.6. Schritt 6/8 - Vorfallsberichte konfigurieren

BitDefender Security for Windows Servers Installation
Übertragung des Installationsprotokolls
BitDefender Security for Windows Servers enthält ein Vorfalls Management Modul, das Ihnen erlaubt bei Produkt-Fehlfunktionen Berichte zu erstellen. Indem Sie zustimmen, die Berichte an das BitDefender Labor zu senden, helfen Sie uns schnelle Lösungen zu finden. Ihr Beitrag könnte helfen ein Stabiles Produkt zu entwickeln, dass Ihren Anforderungen entspricht. Die Berichte werden alleine für das Debugging verwendet und werden niemals für Kommerzielle Zwecke verwendet, oder an Dritte weitergegeben.
Ich bin damit einverstanden Vorfallsberichte an das BitDefender Labor zu senden
Geben Sie eine E-Mail-Adresse an, die als Absender für die Vorfallsberichte verwendet wird.
Klicken Sie auf "Weiter", um mit der Installation zu beginnen.
< Zurück
Weiter >
Abbrechen

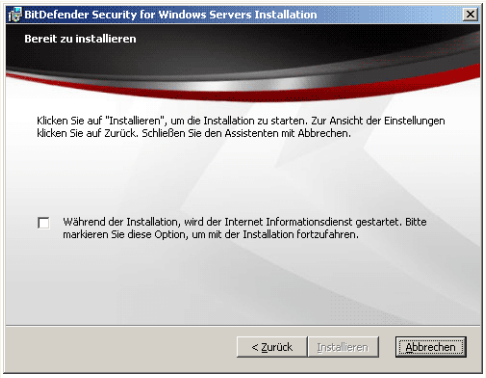
Vorfallsberichte

BitDefener Security für SharePoint enthält einen Vorfall Management Modul, welches es erlaubt während eines Produktabsturzes Berichte zu erstellen. Durch Ihre Zustimmung Vorfallsberichte an das BitDefender Labor zu senden, helfen Sie uns schnelle Problemlösungen zu finden. Sie könnten einen grpssen Beitrag zur der Entwicklung eines stabilen Produktes machen, dass Ihren Wünschen entspricht. Die Berichte werden nur für statistische Zwecke genutzt, die Daten werden niemals kommerziell genutzt oder an dritte weitergegeben.

Um Vorfallsberichte an das BitDefender Labor zu senden, wählen Sie **Ich bin damit einverstanden Berichte an das BitDefender Labor zu senden** und geben Sie Ihre E-Mail-Adresse ein.

Klicken Sie auf **Weiter**.

3.1.7. Schritt 7/8 - Installation starten


BitDefender Security for Windows Servers Installation
Bereit zu installieren
Klicken Sie auf "Installieren", um die Installation zu starten. Zur Ansicht der Einstellungen klicken Sie auf Zurück. Schließen Sie den Assistenten mit Abbrechen.
Während der Installation, wird der Internet Informationsdienst gestartet. Bitte markieren Sie diese Option, um mit der Installation fortzufahren.
< Zurück
Installieren
Abbrechen

Installation starten

BitDefender muss den Internet Informationsdienst während der Installation starten oder wiederherstellen. Sie müssen dem zustimmen, indem Sie das zugehörige Kästchen markieren, bevor der Prozess fortgesetzt werden kann.

Klicken Sie auf **Installieren**, um den Installationsvorgang zu starten.

Es dauert einige Minuten, bis die Installation abgeschlossen ist. Es werden detaillierte Informationen zum Installationsprozess angezeigt, damit Sie ihn nachvollziehen können.

3.1.8. Schritt 8/8 - Installation abgeschlossen

Installation abgeschlossen

Klicken Sie auf **Fertigstellen**, um das Fenster zu schließen. Sie werden möglicherweise aufgefordert, Ihren Computer neuzustarten, damit der Setup-Assistent die Installation beenden kann.

3.2. Bestehende Installation ändern

Um BitDefender Security für SharePoint zu installieren, wenn bereits eine oder mehrere BitDefender Security für Server Produkte auf Ihrem System istalliert sind, müssen Sie diesen Schritten folgen.

1. Wählen Sie im Windows-Startmenü folgenden Eintrag: **Start → Programme → BitDefender Security for Windows Servers → Ändern, Reparieren oder Deinstallieren**.

   Beachten Sie
   Sie können auch auf die Installationsdatei von BitDefender Security for Windows Servers doppelklicken.

   Wenn das Begrüssungsfenster auf geht, klicken Sie **Weiter**, um zu starten.
2. Wählen Sie **Modifizieren**.
3. Sie haben Schritt 4 des Installationsassistenten erreicht. Folgen Sie den Anweisungen des Assistenten, um die Installation fertigzustellen.

3.3. Upgrade für eine ältere Version installieren

Wenn Sie eine ältere Version des Produkts bereits verwenden, können Sie sie auf Version 3.5 aktualisieren, indem Sie den Installer ausführen. Folgen Sie den in *„Neue*

Installation“ (S. 6) beschriebenen Anweisungen des Assistenten, um das Upgrade abzuschließen.

Wenn Sie das Upgrade von Version 3.4 auf 3.5 ausführen, werden alle Einstellungen beibehalten. Upgrades von älteren Versionen werden in der Standardkonfiguration installiert.

Beachten Sie
Das System muss neu gestartet werden, damit das Upgrade abgeschlossen werden kann.

4. BitDefender ändern, reparieren oder entfernen

Wenn Sie BitDefender ändern, reparieren oder entfernen möchten, folgen Sie dem Pfad: **Startmenü → Alle Programme → BitDefender Security for Windows Servers → Ändern, Reparieren oder Entfernen**.

Klicken Sie im Willkommensbildschirm auf **Weiter**. Ein neues Fenster wird erscheinen, in dem Sie folgendes wählen können:

- **Modifizieren** - um neue BitDefender Produkte für Windows Server zu installieren oder um kürzlich installierte Produkte zu entfernen.
- **Reparieren** - um BitDefender Security for SharePoint erneut zu installieren.
- **Entfernen** - dient zum Entfernen aller installierten Komponenten.

BitDefender Security for Windows Servers Installation
Reparire oder Entferne BitDefender
Wählen Sie den Prozess der durchgeführt werden soll.
Ändern
Erlaubt Benutzern, die Art wie Eigenschaften installiert werden, zu ändern.
Reparieren
Repariert Fehler der letzten Installation, repariert fehlende oder beschädigte Dateien, Verknüpfungen und Registry-Einträge.
Entfernen
Entfernt BitDefender Security for Windows Servers von Ihrem Rechner.
< Zurück
Weiter >
Abbrechen

Modifiziere, Reparire oder entferne BitDefender

4.1. Modifiziere BitDefender

Das BitDefender Security for SharePoint Installationspaket ist Teil eines grösseren Packets, dass alle verfügbaren BitDefender Security for Windows Servers Produkte enthält.

Wenn Sie **Modifizieren** wählen, öffnet sich ein neues Fenster, in dem Sie wählen können welche BitDefender Produkte installiert oder entfernt werden sollen.

Sie sollten alle Produkte, die Sie benutzen wollen, zur gleichen Zeit installieren. Um ein Produkt zu installieren, klicken Sie auf den entsprechenden **Pfeil** und klicken Sie dann auf **Wird auf lokaler Festplatte installiert** in dem Shortcut-Menu. Um ein Produkt zu deinstallieren, klicken Sie auf den entsprechenden **Pfeil** und klicken Sie dann auf **Gesamtes Merkmal wird nicht verfügbar sein** in dem Shortcut-Menu.

4.2. BitDefender reparieren

Sollte BitDefender Security for SharePoint sich unerwartet verhalten, können Sie es reparieren, um die Funktionalität wieder her zu stellen. Der Reparaturprozess besteht aus einer Neu-Intsallation des Produktes.

Wenn Sie **Reparieren** wählen, öffnet sich ein neues Fenster. Klicken Sie auf **Reparieren** um die Reparatur zu starten.

Wichtig
Während des Reparaturvorgangs werden alle installierten BitDefender Produkte kurzzeitig aufhören zu funktionieren.

4.3. BitDefender deinstallieren

Wenn Sie alle BitDefender Produkte deinstallieren wollen, wählen Sie **Entfernen**.

Beachten Sie
Wir empfehlen die Option **Entfernen** zu verwenden um eine saubere Neuinstallation durchzuführen.

Wenn Sie BitDefender entfernen wählen erscheint ein neues Fenster. Damit die Objekte in der Quarantäne zu bleiben, darf das entsprechende Kästchen nicht markiert sein. Klicken Sie auf **Entfernen** um BitDefender von Ihrem Computer zu entfernen.

Wichtig
Dies wird alle BitDefender Security für Windows Server Produkte von ihrem Computer entfernen. Wenn Sie weitere BitDefender Produkte installiert haben und nur BitDefender Security für SharePoint deinstallieren wollen, Benutzen Sie bitte die Modifizieren" Option.

Konfiguration und Verwaltung

5. Erste Schritte

BitDefender Security für SharePoint Server integriert sich nahtlos in Microsoft Office SharePoint Server 2007. Die Management-Konsole bietet Zugriff auf alle Funktionen und Einstellungen von BitDefender Security for SharePoint.

Um die Management Konsole zu öffnen, folgen Sie diesen Schritten:

1. Greifen Sie auf die zentrale Verwaltungsseite von Microsoft Office ScharePoint Server 2007 zu.
2. Klicken Sie auf der oberen Navigationsleiste auf **Ablauf**
3. Auf der **Ablauf** Seite,unter **BitDefender**, klicke **BitDefender Security für SharePoint**.

Beachten Sie
Alternativ können Sie diesem Pfad vom Windows-Startmenü folgen:**Start → Alle Programme → BitDefender Security for Windows Servers → BitDefender Security für SharePoint**.

Auf dem oberen Teil der Seite sehen Sie das BitDefender Menu:

- Home - Zeigt das Dashboard an.

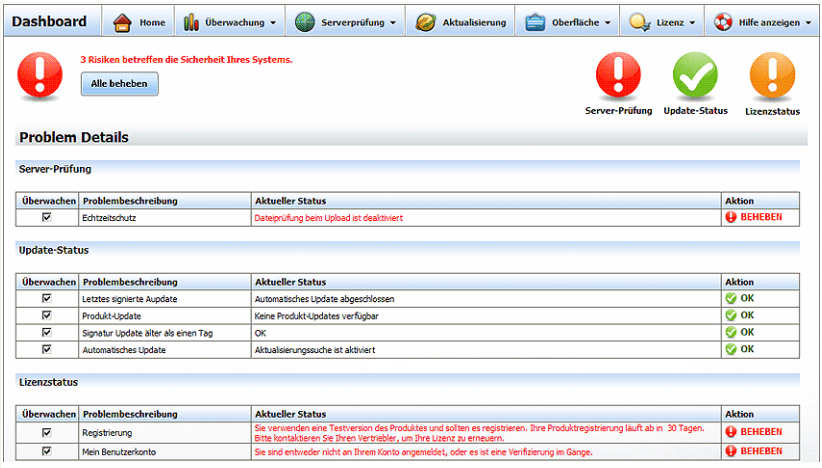
  Das Dashboard gibt Ihnen nützliche Informationen über den Status von BitDefender Security for SharePoint und hilft Ihnen dabei Probleme einfach zu lösen.

- Monitoring - bietet Links zu den folgenden Abschnitten:
  - Statistiken - bietet einen statistischen Überblick über die Produktaktivität.
  - Berichte - dient zum Erstellen von benutzerdefinierten Berichten über die Produktaktivität.
  - Benachrichtigungen & Protokolle - bietet die Möglichkeit die Protokolloptionen zu konfigurieren und Benachrichtigungen über die Ereignisse, die während des Betriebs des Produktes auftraten (wie ein Update-Fehler oder der Fund einer infizierten Datei), zu senden.
  - Quarantäne - zeigt die Dateien an, die sich in der Quarantäne befinden. Diese Dateien wurden als infiziert oder verdächtig erkannt und wurden entsprechend der festgelegten Aktion in den Quarantäneordner verschoben.
  - Geplante Aufgaben - dient zur Einrichtung zeitgesteuerter Aufgaben mithilfe eines hilfreichen Assistenten. Sie können Updates, On-Demand Prüfprozesse und die Erstellung von Berichten planen.
- Server Scan - erlaubt BitDefender den Server zu prüfen.
- Update - BitDefender kann aktualisiert und Update-Einstellungen können konfiguriert werden.
- Allgemein - BitDefender kann so konfiguriert werden, dass zu dem BitDefender Labor Berichte bezüglich der Viren gesendet werden, die auf dem Server gefunden wurden sowie über Vorfälle während des Produktbetriebs.

- Lizenz - ermöglicht die Registrierung von BitDefender, Erstellung eines BitDefender Kontos und Zugriff auf eine Webseite von der aus Sie BitDefender kaufen können.
- Help - ermöglicht es Ihnen Hilfe und Support zu holen und Versionsinformationen abzurufen.

6. Dashboard

Um das dashboard zu sehen, klicken Sie **Home** im BitDefender Menu.



Dashboard

Das Dashboard gibt Ihnen nützliche Informationen über den Status von BitDefender Security for SharePoint und hilft Ihnen dabei Probleme einfach zu lösen. Sie sollten das Dashboard regelmäßig überprüfen, um Probleme, die die Sicherheit des Server betreffen, schnell lösen zu können.

6.1. Statusbereich

Die **Status** Bereich enthält Informationen über existierende Probleme und hilft Ihnen diese zu beseitigen.

Drei Statusschaltflächen, die drei Problemkategorien überwachen, informieren Sie direkt über das Vorhandensein bestimmter Probleme:

- Server-Prüfung
- Update-Status
- Lizenz-Status

Beachten Sie
Die Schaltfläche Lizenzstatus und die dazugehörenden Angelegenheiten sind nicht verfügbar, wenn BitDefender Security für SharePoint vom BitDefender Management Server verwaltet wird.

Auf der linken Seite der Statusschaltflächen können Sie die Anzahl der Probleme sehen, die die Sicherheit des File Servers betreffen (falls vorhanden).

Die Schaltflächen können je nach Sicherheitsstatus des Servers die Farben grün, rot oder grau annehmen:

- Wenn die Status-Schaltflächen **Grün** aufleuchten, gibt es nichts, worüber Sie sich Sorgen machen müssten.
- **Gelb** signalisiert ein mittleres Sicherheitsrisiko für Ihren Computer. Diese Probleme verlangen zwar keine direkte Aufmerksamkeit, doch sollten Sie sich so bald wie möglich mit Ihnen befassen.
- Wenn die Status-Schaltflächen **Rot** aufleuchten, wird die Anwesenheit eines wichtigen Sicherheitsrisikos angezeigt, das Ihre direkte Aufmerksamkeit erfordert.

Details über diese Angelegenheiten, werden im Bereich **Details** angezeigt.

Der Abschnitt **Vorfalls-Details** enthält drei Tabellen, eine für jede Kategorie. Jede Tabelle zeigt die überwachten Objekte und deren aktuellen Status an. Wenn ein Problem eines der überwachten Objekte betrifft, wird ein roter Link **Beheben** angezeigt. Klicken Sie entweder auf die **Beheben**-Schaltfläche, um ein Risiko nach dem anderen zu beheben oder verwenden Sie die Schaltfläche **Alle beheben** um alle auf einmal zu beheben.

Wichtig

Für jedes überwachte Objekt gibt es ein Kontrollkästchen, das in der Spalte **Überwachen** standardmäßig markiert ist. Wenn Sie möchten, dass ein bestimmtes Objekt nicht überwacht wird, deaktivieren Sie das entsprechende Kontrollkästchen.

6.1.1. Serverprüfung

Wenn die Schaltfläche für die Server-Prüfung rot oder gelb ist, betreffen Probleme die Prüfaktivität von BitDefender Security für SharePoint.

Prüfen Sie die **Server scan** Tabelle, um den aktuellen Status des **Echtzeit Schutzes** zu sehen.

Die Probleme, die angezeigt werden können sind in der folgenden Tabelle aufgeführt:

Status	Beschreibung
Dateien prüfen deaktiviert	Der Echtzeitschutz ist deaktiviert und der Server ist nicht gegen Malware geschützt. Klicken Sie auf **Beheben** - um den Echtzeitschutz zu aktivieren.
Dateiprüfung beim Upload / Download ist deaktiviert	Echtzeitschutz ist aktiviert, aber die Prüfung der Dateien beim Upload / Download wurde von der Microsoft SharePoint Antivirus Einstellingsseite deaktiviert. Klicken Sie **Reparieren**, um die Dateiprüfung beim Upload / Download zu aktivieren.

Status	Beschreibung
Versuch infizierte Dokumente zu säubern is deaktiviert	Diese Eigenschaft ist auf der Microsoft SharePoint Antivirus Einstellungsseite deaktiviert. Klicke **beheben**, um es einzuschalten.
Die Registrierung ist abgelaufen**Fix**	Der Lizenzzeitraum ist abgelaufen. Klicken Sie auf **Beheben** um den Registrierungsassistenten zu öffnen und BitDefender Security für SharePoint mit einem neuen Lizenzschlüssel zu registrieren.

6.1.2. Update Status

Eine gelbe oder rote Schaltfläche des Update-Status signalisieren Update-Probleme, die BitDefender Security für SharepPoint betreffen.

Überprüfen Sie den **Update Status** Tabelle, um die überwachten Komponenten und ihren Status zu beobachten.

- **Letzter Signaturupdate Status.** Die Probleme, die angezeigt werden können sind in der folgenden Tabelle aufgeführt:

Status	Beschreibung
Mindestens eine Update Location ist fehlgeschlagen (AV Update Location / Produkt Update Location)	Einen oder beide Update Locations konnten während des letzten Signatur- und/oder Produktupdates nicht erreicht werden. Klicken Sie auf **Beheben** um ein neues Update zu starten.
Kein Update durchgeführt	Klicken Sie auf **Beheben** um ein neues Update zu starten. Der Status wechselt dann auf **Lade herunter**.
Update fehlgeschlagen, da die Updates auf Ihrem Server nicht signiert sind und Sie gewählt haben nicht signierte Updates nicht zu erlauben	Gehen Sie zu Update > Locations und markieren Sie **Unsignierte Updates erlauben** für Ihren Server.

- **Letzte Produktaktualisierung.** Die Probleme, die angezeigt werden können sind in der folgenden Tabelle aufgeführt:

Status	Beschreibung
Automatische Produktupdates sind deaktiviert	Automatische Produktupdates sind deaktiviert. Dies macht Ihren Server angreifbarer für Sicherheitsbedrohungen. Klicken Sie auf **Beheben** um das automatische Update zu aktivieren.

Status	Beschreibung
Ein neues Paket ist verfügbar und nicht auf Ihrem System installiert	Das neue Paket verfügt möglicherweise über neue Funktionen. Klicke **Beheben**, um das Kit herunterzuladen und zu installieren. Sie werden aufgefordert, Ihre Auswahl zu bestätigen. Klicken Sie dazu auf **OK**. Die Installation des Kits könnte einen Server Neustart erfordern.
Produktupdate wurde heruntergeladen, bitte installieren Sie es	Ein Produktupdate wurde heruntergeladen, aber noch nicht installiert. Klicken Sie auf**Beheben**, um das Update zu installieren.

- **Status für Updates, die älter als ein Tag sind.** Die Probleme, die angezeigt werden können sind in der folgenden Tabelle aufgeführt:

Status	Beschreibung
Updates sind alt	Mehr als ein Tag ist seit dem letzten Update vergangen Klicken Sie auf **Beheben** um ein neues Update zu starten. Der Status wechselt dann auf **Lade herunter**.

- **Staus des automatischen Update.** Die Probleme, die angezeigt werden können sind in der folgenden Tabelle aufgeführt:

Status	Beschreibung
Automatisches Update ist deaktiviert und keine geplante Update-Aufgabe ist festgelegt oder aktiviert	BitDefender Security for SharePoint wird nicht automatisch regelmäßig aktualisiert. Klicken Sie auf **Beheben** um das automatische Update zu aktivieren. Wenn nicht anders konfiguriert, wird das Update-Intervall auf eine Stunde eingestellt.

6.1.3. Lizenzstatus

Eine gelbe oder rote Schaltfläche bei dem Lizenzstatus signalisieren Angelegenheiten bezüglich der Lizenz Ihres BitDefender Security für SharePoint.

Beachten Sie

Die Schaltfläche Lizenzstatus und die dazugehörenden Angelegenheiten sind nicht verfügbar, wenn BitDefender Security für SharePoint vom BitDefender Management

Server verwaltet wird. In diesem Fall wird die Registrierung von der Management-Konsole des BitDefender Management Server durchgeführt.

Überprüfen Sie die **Lizenz Status** Tabelle, um die überwachten Komponenten und ihren Status zu beobachten.

- **Status der Registrierung.** Die Probleme, die angezeigt werden können sind in der folgenden Tabelle aufgeführt:

Status	Beschreibung
Sie benutzen eine Testversion des Produktes und sollten es registrieren	Der Status wird während der Testzeit angezeigt. Klicken Sie auf **Beheben** um den Registrierungsassistenten zu öffnen und BitDefender Security für SharePoint mit einem neuen Lizenzschlüssel zu registrieren.
Die Seriennummer, die Sie eingegeben haben, ist ungültig!	Sie haben einen ungültigen Lizenzschlüssel eingegeben. Klicken Sie auf **Beheben** um den Registrierungsassistenten zu öffnen und BitDefender Security für SharePoint mit einem neuen Lizenzschlüssel zu registrieren.
Ihre Produktregistrierung wird in x Tagen ablaufen. Sie sollten Ihre Registrierung erneuern	Der Status wird während der letzten 30 Tage des Lizenzzeitraums angezeigt. Klicken Sie auf **Beheben** um den Registrierungsassistenten zu öffnen und BitDefender Security für SharePoint mit einem neuen Lizenzschlüssel zu registrieren.
Produktregistrierung abgelaufen	Der Lizenzzeitraum ist abgelaufen. Klicken Sie auf **Beheben** um den Registrierungsassistenten zu öffnen und BitDefender Security für SharePoint mit einem neuen Lizenzschlüssel zu registrieren.

- **Status für Mein Benutzerkonto.** Die Probleme, die angezeigt werden können sind in der folgenden Tabelle aufgeführt:

Status	Beschreibung
Sie haben kein Benutzerkonto. Bitte erstellen Sie ein Konto.	Sie haben noch kein Benutzerkonto registriert. Klicken Sie **Beheben** um den Link zur Mein Konto Seite zu öffnen. Dort können Sie neues Konto eröffnen oder Sich an einem existierenden anmelden.
Das Passwort ist falsch. Versuchen Sie es erneut.	Klicken Sie **Beheben** um den Link zur Mein Konto Seite zu öffnen. Dort können Sie neues Konto eröffnen oder Sich an einem existierenden anmelden.

Status	Beschreibung
Benutzerkonto gesperrt	Klicken Sie **Beheben** um den Link zur Mein Konto Seite zu öffnen. Dort können Sie neues Konto eröffnen oder Sich an einem existierenden anmelden.
Server Fehler. Bitte versuchen Sie es später nochmal	Eine Verbindung zum BitDefender Server konnte nicht hergestellt werden. Klicke **Beheben**, um die Mein Konto Seite zu öffnen und versuche Sie es später erneut.

- **Benachrichtigung für Registrierung wird ablaufen.** Der Status dieses Objekts sich kann wie in der folgenden Tabelle gezeigt verändern:

Status	Beschreibung
In x Tagen läuft Ihr Lizenzschlüssel ab.	Der Status wird während der letzten 30 Tage des Lizenzzeitraums angezeigt. Klicken Sie auf **Beheben** um den Registrierungsassistenten zu öffnen und BitDefender Security for SharePoint mit einem neuen Lizenzschlüssel zu registrieren.
Produkt abgelaufen	Der Lizenzzeitraum ist abgelaufen. Klicken Sie auf **Beheben** um den Registrierungsassistenten zu öffnen und BitDefender Security for SharePoint mit einem neuen Lizenzschlüssel zu registrieren.

6.2. Produkt-Status

Die Information über den Produktstatus ist im **Produkt Status** Abschnitt zu sehen.

Sie können den Namen des Servers sehen, auf dem BitDefender Security für SharePoint installiert ist, sowie die Produktversion und die Anzahl der verfügbaren Malware-Signaturen.

7. Überwachung

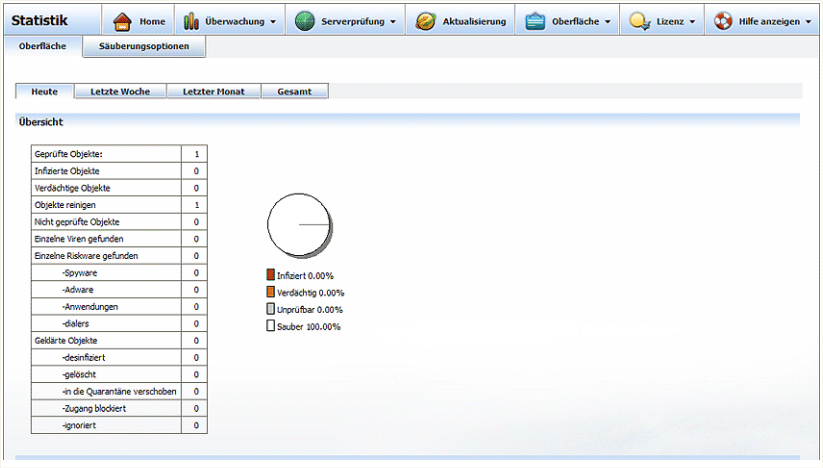
Das Monitoring Menu stellt Ihnen all nötigen Mittel zur Verfügung die Produktaktivität zu überwachen und kontrollieren. Die folgenden Abschnitte sind unter Montioring gruppiert:

- Statistiken - bietet einen statistischen Überblick über die Produktaktivität.
- Berichte - dient zum Erstellen von benutzerdefinierten Berichten über die Produktaktivität.
- Benachrichtigungen & Protokolle - bietet die Möglichkeit die Protokolloptionen zu konfigurieren und Benachrichtigungen über die Ereignisse, die während des Betriebs des Produktes auftraten (wie ein Update-Fehler oder der Fund einer infizierten Datei), zu senden.
- Quarantäne - zeigt die Dateien an, die sich in der Quarantäne befinden. Diese Dateien wurden als infiziert oder verdächtig erkannt und wurden entsprechend der festgelegten Aktion in den Quarantäneordner verschoben.
- Geplante Aufgaben - dient zur Einrichtung zeitgesteuerter Aufgaben mithilfe eines hilfreichen Assistenten. Sie können Updates, On-Demand Prüfprozesse und die Erstellung von Berichten planen.

In diesem Kapitel finden Sie eine detaillierte Beschreibung über jeden Bereich.

7.1. Statistik

Wenn Sie detaillierte Statistiken über die Aktivität der Echtzeitprüfung von BitDefender Security für SharePoint sehen wollen, klicken sie auf **Statistiken** unter **Monitoring** im BitDefender Menu.



Statistik

BitDefender speichert Daten über die geprüften Objekte in Echtzeit auf eine Datenbank. Indem diese Datenbank verwendet wird, kann BitDefender detaillierte Statistiken liefern, mit denen Sie Folgendes einschätzen können:

- der Sicherheitsstatus des SharePoint Servers.
- die bestehenden Bedrohungen und deren Gefahrenpotenzial.

Folgende Arten von Statistiken stehen zur Verfügung:

Typ	Beschreibung
Zusammenfassung	Bietet allgemeine Statistiken über die Echtzeit Prüfaktivität von BitDefender Security für SharePoint: ● Anzahl der geprüften Objekte. ● Anzahl der gefundenen infizierten/verdächtigen/sauberen Objekte. ● Anzahl der Objekte, die nicht geprüft werden konnten. ● Anzahl der entdeckten Viren. ● Anzahl der entdeckten Riskware, sowohl insgesamt als auch nach Riskware-Typ geordnet.

Typ	Beschreibung
	• Anzahl der gelösten Probleme, sowohl insgesamt als auch nach Aktionstyp geordnet. Ein Kreisdiagramm zeigt die Prozentzahl infizierter, verdächtiger, nicht prüfbarer und sauberer Dateien an. Gemeinsam stellen diese die gesamte Anzahl der geprüften Dateien dar.
Top Malware	Zeigt die 10 am häufigsten entdeckten Malwares. Die Statistiken sind auf dem unteren Seitenabschnitt verfügbar.

Die Statistiken sind in 4 Zeitintervalle unterteilt: heute, letzte Woche, letzter Monat und insgesamt. Um Statistiken zu öffnen klicken Sie auf den entsprechenden Link.

Beachten Sie

Die Statistiken werden alle 60 Sekunden aktualisiert um Sie mit Informationen in Echtzeit zu versorgen.

7.1.1. Statistiken säubern

Standardmäßig löscht BitDefender statistische Informationen, die älter als 30 Tage sind. Um den Zeitraum zu ändern, in dem Statistiken gespeichert werden, gehen Sie zu **Löschoptionen** auf der**Statistik** Seite.

In dem Bearbeiten Feld geben Sie ein wieviele Tage / Wochen / Monate statistische Informationen gespeichert werden sollen und klicken Sie **Anwenden**, um die Änderungen zu speichern.

Um die Statistiken manuell zu löschen, wähle **Alle Statistiken jetzt löschen** und klicke **Anwenden**.

Beachten Sie

Berichte und Statistiken werden mithilfe der gleichen Datenbank erstellt. Das Säubern der Statistiken hat also auch Auswirkungen auf die Genauigkeit der Berichte.

7.2. Berichte

Mit BitDefender können Berichte über die Prüfaktivität in einen bestimmten Zeitraum erstellt werden. Diese Berichte können sehr nützlich sein, sie können ausgedruckt und an Andere weitergesendet werden, die sich für den Status der Sicherheit des Servers interessieren.

Berichte können im HTML- oder im CSV-Format erstellt werden. Folgende Berichttypen können erstellt werden:

Berichttyp	Beschreibung
Antivirus Gesamt	Bietet umfangreiche Informationen über die Bedrohungen die innerhalb eines bestimmten Zeitraums entdeckt wurden.
Häufigste Viren	Bietet eine Tabelle mit den entdeckten Bedrohungen, die innerhalb eines bestimmten Zeitraums entdeckt wurden, geordnet nach der Anzahl der infizierten Dateien.

Die Berichte sind im Ordner `C:\Programme\BitDefender\BitDefender Security für SharePoint\Berichte` gespeichert.

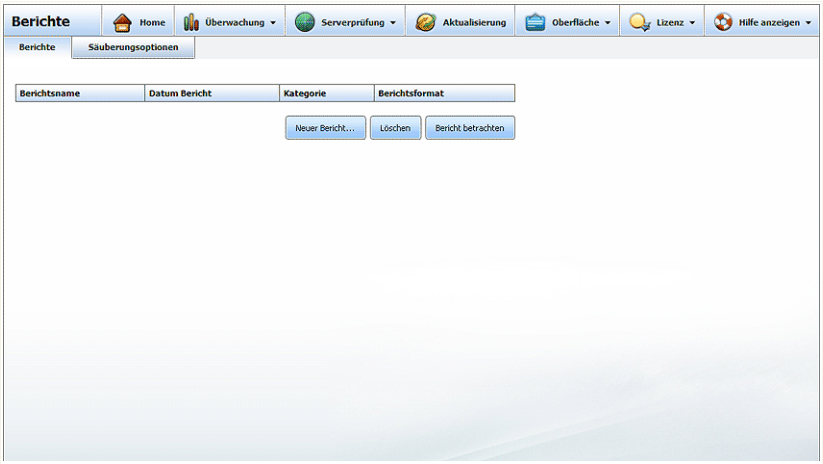
Beachten Sie

Berichte werden anhand der Informationen erstellt, die sich in der BitDefender Datenbank befinden, die standardmäßig einmal pro Woche gesäubert wird. Wenn Berichte während des Zeitraums gelöscht werden, die vom Bericht selbst abgedeckt werden, so können die gelieferten Informationen ungenau sein.

Um Berichte zu erstellen, zu betrachten und zu verwalten, klicken Sie auf **Berichte** im Baummenu (unter **Überwachen**).

Wichtig

In dem Bereich **Berichte** finden Sie auch die On-Demand Prüfberichte.



Berichte

Alle existierenden Berichte sind in der Tabelle aufgelistet. Für jeden Bericht werden folgende Informationen angezeigt: Name des Berichts, Datum der Erstellung des Berichts, die Art der beinhalteten Informationen und das Format.

7.2.1. Berichte verwalten

Verwenden Sie die zur Verfügung stehenden Schaltflächen um Berichte zu verwalten.

- **Neuer Bericht** - startet den Assistenten, der Ihnen beim Erstellen eines neuen Berichtes hilft.
- **Löschen** - löscht einen oder mehrere ausgewählte Berichte.
- **Bericht anzeigen** - öffnet den ausgewählten Bericht.

7.2.2. Berichte erstellen

Um Berichte über die Produktaktivität zu erstellen, klicken Sie auf **Neuer Bericht** und führen Sie den Assistenten durch.

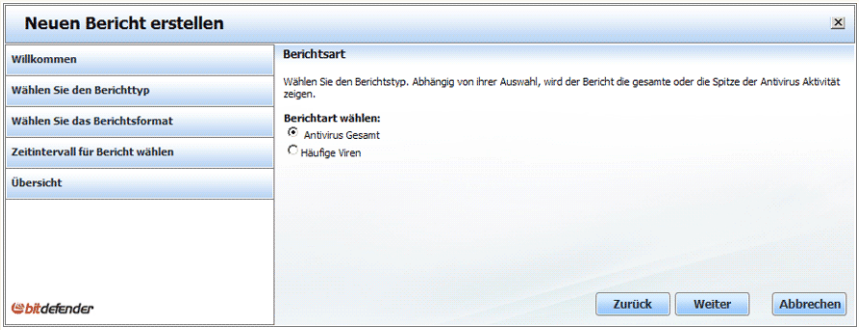
Schritt 1/5 - Willkommen beim Berichtassistenten.

Neuen Bericht erstellen
Willkommen
Wählen Sie den Berichttyp
Wählen Sie das Berichtsformat
Zeitintervall für Bericht wählen
Übersicht
bitdefender
Willkommen zum BitDefender Security for SharePoint Berichtassistenten.
Der Berichtassistent führt Sie durch die notwendigen Schritte, um einen Bericht über die Aktivität des BitDefender Security for SharePoint Servers zu erstellen, das auf dem Server installiert ist.
Weiter
Abbrechen

Willkommen

Klicken Sie auf **Weiter**.

Schritt 2/5 – Berichttyp wählen



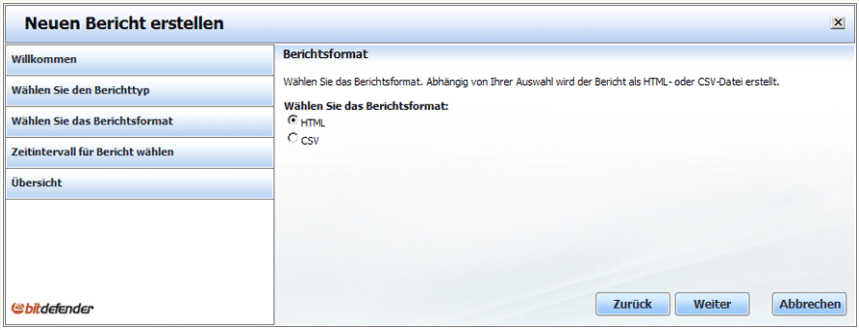
Wählen Sie den Berichttyp

Wählen Sie eine der zur Verfügung stehenden Berichttypen.

Berichttyp	Beschreibung
Antivirus Gesamt	Bietet umfangreiche Informationen über die Bedrohungen die innerhalb eines bestimmten Zeitraums entdeckt wurden.
Häufigste Viren	Bietet eine Tabelle mit den entdeckten Bedrohungen, die innerhalb eines bestimmten Zeitraums entdeckt wurden, geordnet nach der Anzahl der infizierten Dateien.

Klicken Sie auf **Weiter**.

Schritt 3/5 – Berichtsformat wählen



Wählen Sie das Berichtsformat

Wählen Sie das Format der Berichtdatei (**HTML** oder **CSV**).

Klicken Sie auf **Weiter**.

Schritt 4/5 – Zeitraum auswählen

Wählen Sie den Zeitraum aus

Wählen Sie den im Bericht bedeckten Zeitabstand aus:

- **Letzter Tag**
- **Letzte Woche**
- **Letzter Monat**
- **Benutzerdefiniert**

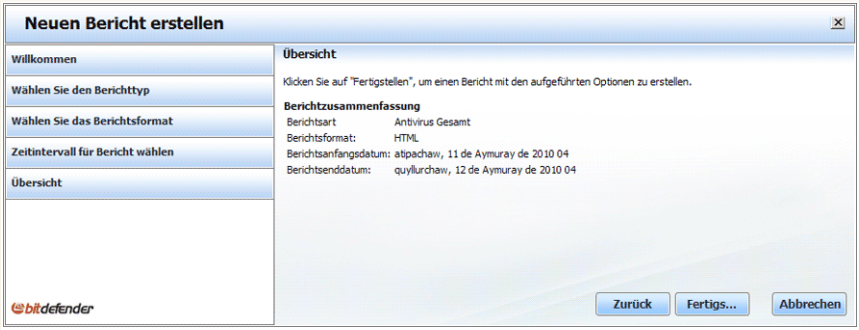
Wenn Sie Information über BitDefender mit einem spezifischen Zeitabstand verbundene Tätigkeit benötigen, wählen Sie **anpassen** und geben Sie das Beginn/Endedatum an. Um Anfangs und Enddaten festzulegen, geben Sie entweder neue Werte in die Datumsfelder oder klicken Sie das Kalender Symbol und wählen Sie Daten vom Kalender.

Beachten Sie
Das Format des Datums ist Monat/Tag/Jahr.

Nur Aufnahmen aus dem festgelegten Zeitraum werden in dem Bericht erscheinen.

Klicken Sie auf **Weiter**.

Schritt 5/5 – Zusammenfassung betrachten



Betrachten Sie die Zusammenfassung

In diesem Fenster können Sie die getätigten Berichteinstellungen überprüfen. Sie können alle Änderungen vornehmen, indem Sie zu den vorigen Schritten zurück gehen. Um dies zu tun, klicken Sie **Zurück** um zum vorigen Schritt zurück zu gehen, oder wählen Sie irgendeinen Schritt in der linken Fensterhälfte.

Klicken Sie auf **Beenden**, um den Bericht zu erstellen. Der Bericht wird nun im Bereich Berichte angezeigt.

7.2.3. Berichte löschen

Um den Zeitraum zu ändern, in dem Statistiken gespeichert werden, gehen Sie zu **Löschoptionen** auf der**Statistik** Seite. Geben Sie die Anzahl der Stunden / Tage / Wochen / Monate für die Aufbewahrung ein und klicken Sie auf **OK** um die Änderungen zu speichern.

Um die Statistiken manuell zu löschen, wähle **Alle Statistiken jetzt löschen** und klicke **Anwenden**.

Beachten Sie
Berichte, die älter als der angegebene Zeitraum sind, werden automatisch gelöscht.

7.3. Benachrichtigungen & Protokolle

Mit **Benachrichtigungen & Protokolle** können Sie das Benachrichtigungssystem von BitDefender konfigurieren.

BitDefender ist standardmäßig so konfiguriert, dass die Aktivität protokolliert wird. Das BitDefender Protokoll liefert Ihnen eine umfangreiche Liste der Ereignisse, die während des Produktbetriebs aufgetreten sind. Um die Protokollierung zu konfigurieren oder die Protokolldateien zu betrachten, öffnen Sie den Tab Protokolle

Weiterhin können Sie Bitdefender so konfigurieren, dass bestimmte Benutzer sofort benachrichtigt werden, wenn bestimmte Ereignisse während des Produktbetriebs auftreten. Benachrichtigungen können mit dem Befehl`Net Send` gesendet werden. Sie können Benachrichtigungen für jedes Ereignis vollständig deaktivieren oder Sie können BitDefender so konfigurieren, dass Mail- und Net Send Benachrichtigungen gesendet werden, wenn das Ereignis auftritt. Um Benachrichtigungen für jeden Vorfall zu konfigurieren, gehen Sie zum Alerts tab.

Beachten Sie
Windows Server 2008 unterstützt keine Net Send Benachrichtigungen.

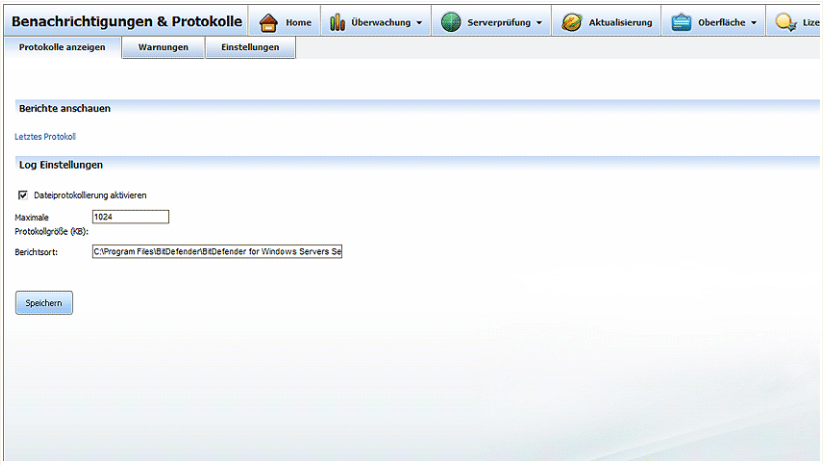
Um die Mail- und Net Send Benachrichtigungsdienste zu konfigurieren, öffnen Sie den Tab Einstellungen

7.3.1. Protokolle

BitDefender ist standardmäßig so konfiguriert, dass die Aktivität protokolliert wird. Das BitDefender Protokoll liefert Ihnen eine umfangreiche Liste der Ereignisse, die während des Produktbetriebs aufgetreten sind.

Beachten Sie
Standardmässig wird die Berichtsdatei gespeichert unter: `?:\Programme\BitDefender\BitDefender für Windows Servers Services\BDLog`.

Um die Protokollierung zu Konfigurieren und die Protokolldateien zu sehen, gehen Sie zu **Benachrichtigungen & Protokolle** unter **Monitoring** im BitDefender Menu.



Protokolle

Protokolle prüfen

Klicken Sie auf **Letztes Protokoll anzeigen**, um die letzte Protokolldatei zu öffnen.

Protokollierung konfigurieren

Um die Produktaktivität in einer Datei zu protokollieren, wählen Sie **Dateiprotokollierung aktivieren**.

BitDefender erstellt die Protokolldatei in `?:\Programme\BitDefender\BitDefender für Windows Servers Services\BDLog`. Wenn die Datei die Größe von 1024 KB erreicht, wird standardmäßig eine neue Protokolldatei erstellt.

Legen Sie das Größenlimit der Protokolldateien in dem Feld **Maximale Größe von Protokolldateien** fest. Wenn Sie keine Beschränkung möchten, geben Sie 0 in das Feld ein.

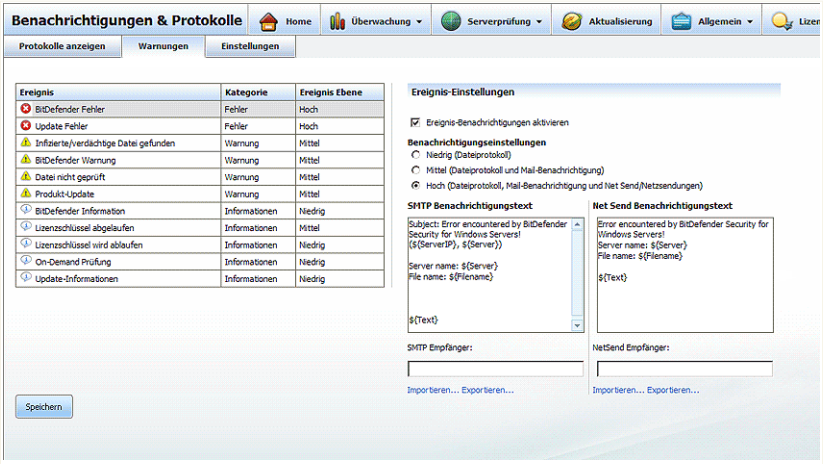
Sie können einen alternativen Ordner angeben, wo die Dateien gespeichert werden, indem Sie den Pfad in das zugehörige Feld eingeben.

Klicken Sie **Speichern**, um die Änderungen zu speichern.

7.3.2. Benachrichtigungen

Sie können Benachrichtigungen für jedes Ereignis vollständig deaktivieren oder Sie können BitDefender so konfigurieren, dass Mail- und Net Send Benachrichtigungen gesendet werden, wenn das Ereignis auftritt.

Um die Banchrichtigungsmethoden für jeden Vorfall festzulegen, gehen Sie zu **Benachrichtigungen & Protokolle** unter **Monitoring** im BitDefender Menu und dann gehen Sie zu **Benachrichtigungen**.



Benachrichtigungen

Alle möglichen Ereignisse sind in der Tabelle aufgelistet. Es gibt 3 mögliche Ereignisse:

- **Information** - diese Ereignisse liefern Informationen über die Produktaktivität.
- **Warnung** - diese Ereignisse liefern wichtige Informationen über die Produktaktivität und erfordern Ihre Aufmerksamkeit.
- **Fehler** - diese Ereignisse liefern Informationen über Fehler die während des Produktbetriebs aufgetreten sind.

Hier ist die Liste der Ereignisse die auftreten können:

Ereignis	Beschreibung
BitDefender Fehler	Unterteilt alle Fehler, die während des Produktbetriebs auftreten können, so wie das Fehlschlagen des Starts.
Update-Fehler	Informiert über das Auftreten eines Fehlers während des Update-Prozesses.

Ereignis	Beschreibung
Infizierte/verdächtige Datei entdeckt	Geschieht wenn eine infizierte Datei or vermutlich infizierte Datei gefunden wird.
BitDefender Warnung	Unterteilt wichtige Informationen über die Aktivität von BitDefender.
Datei nicht geprüft	Erscheint wenn eine Datei nicht von Bitdefender geprüft werden konnte.
Produkt-Update	Erscheint wenn ein Update zur Verfügung steht.
BitDefender Information	Enthält Informationen über die Aktivität von BitDefender.
Lizenzschlüssel abgelaufen	Zeigt den Ablauf des Registrierungszeitraums an.
Lizenzschlüssel wird ablaufen	Zeigt an, dass noch 3 Tage verbleiben, bis die Lizenz abläuft.
On-Demand Prüfung	Erscheint wenn eine On-Demand Prüfung durchgeführt wird.
Update-Information	Enthält Informationen über den Update-Prozess.

Ereignisse konfigurieren

Sie können die Benachrichtigungsmethoden für jedes Ereignis in der Liste seperat konfigurieren. Um die Benachrichtigungen für ein bestimmtes Ereignis anzupassen, wählen sie es und ändern Sie die verfügbaren Optionen in den **Ereigniseinstellungen** in der rechten Seite des Fensters.

Benachrichtigungen Aktivieren/Deaktivieren

Um Benachrichtigungen für eine oder mehrere ausgesuchte Ereignisse zu aktivieren/deaktivieren, wähle/lösche das entsprechende Kästchen.

Beachten Sie
Wenn die Ereignisbenachrichtigung deaktiviert ist, wird das Ereignis nicht protokolliert und keine Benachrichtigung wird gesendet.

Ereigniswichtigkeit auswählen

Stellen Sie die Wichtigkeit des Ereignisses unter **Benachrichtigungseinstellungen** ein:

- **Niedrig** - Ein Bericht des Ereignisses wird in der Protokoll Datei gespeichert. Es wird keine Benachrichtigung gesendet, wenn das Ereignis stattfindet.
- **Mittel** - Protokolliere das Ereignis und sende E-Mail Benachrichtigungen, wenn das Ereignis stattfindet.
- **Hoch** - Protokolliere das Ereignis und sende sowohl E-Mail als auch Net Send Benachrichtigungen, wenn das Ereignis stattfindet.

Mail-Benachrichtigungen konfigurieren

Wenn die Wichtigkeit des Ereignisses mittel oder hoch ist, werden Mail-Benachrichtigungen gesendet. Sie können den Benachrichtigungstext ändern und die Empfänger bestimmen.

Klicken Sie **Speichern**, um die Änderungen zu speichern.

- Jedes Ereignis hat einen standard Benachrichtigungstext, welches im **SMTP Benachrichtigungstext** angezeigt wird. Um den Text zu ändern, ändern Sie den Inhalt des Textfeldes.

  Wichtig
  Sie sollten die Zeichenfolgen, die mit dem Symbol `$` beginnen nicht verändern, da diese wichtige Informationen über das Ereignis liefern.

- Benachrichtigungen werden standardmässig an die Adressen gesendet, die in Einstellungen definiert sind. Geben Sie zusätzliche E-Mail Adressen im Feld **SMTP Empfänger**, um Empfänger zur Liste hinzuzufügen. Adressen müssen durch Kommata (",") oder Semikolon (";") getrennt werden.

  Um eine E-Mail-Adresse aus einer `txt` Datei zu importieren, klicken Sie auf **Importieren...**, wählen Sie die Datei und klicken Sie auf **Öffnen**. Wenn Sie die Liste in eine `txt` Datei esportieren wollen, klcken Sie **Exportieren...**, wählen Sie einen Ort und klicken Sie **Speichern**.

Net Send Benachrichtigungen konfigurieren

Wenn die Wichtigkeit des Ereignisses hoch ist, werden Net Send Benachrichtigungen gesendet. Sie können den Benachrichtigungstext ändern und die Empfänger bestimmen.

- Jedes Ereignis hat einen standard Benachrichtigungstext, welcher im **Net Send Benachrichtigungstext** angezeigt wird. Um den Text zu ändern, ändern Sie den Inhalt des Textfeldes.

  Wichtig
  Sie sollten die Zeichenfolgen, die mit dem Symbol `$` beginnen nicht verändern, da diese wichtige Informationen über das Ereignis liefern.

- Benachrichtigungen werden standardmässig an die Adressen gesendet, die in Einstellungen definiert sind. Geben Sie zusätzliche E-Mail Adressen im Feld **SMTP Empfänger**, um Empfänger zur Liste hinzuzufügen. Computernamen müssen durch ein Komma (",") oder Semikolon (";) getrennt werden.

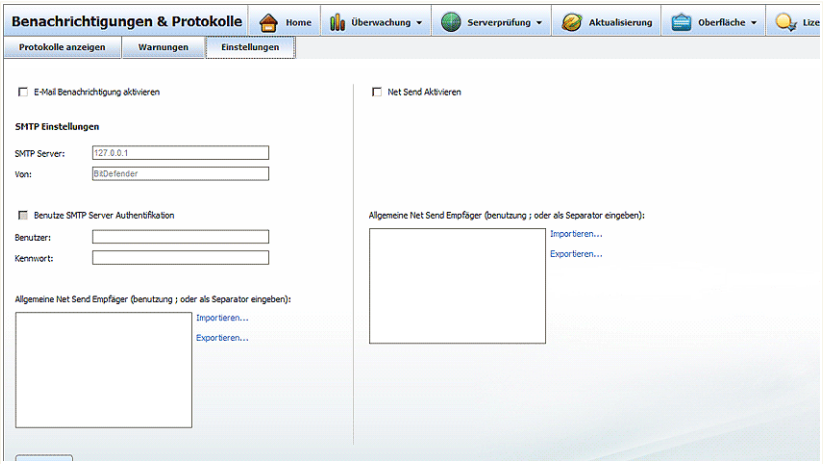
  Um Computernamen aus einer `txt` Datei zu importieren, klicken Sie auf **Importieren...**, wählen Sie die Datei aus und klicken Sie dann auf **Öffnen**. Wenn Sie die Liste in eine `txt` Datei esportieren wollen, klcken Sie **Exportieren...**, wählen Sie einen Ort und klicken Sie **Speichern**.

Klicken Sie **Speichern**, um die Änderungen zu speichern.

7.3.3. Benachrichtigungseinstellungen

Benachrichtigungen sind Nachrichten, die produktbezogene Informationen beinhalten und die Empfänger über die Produktaktivität informieren sollen. BitDefender kann so eingestellt werden, dass Benutzer und Administratoren über Mail oder Net Send über auftretende Ereignisse benachrichtigt werden.

Um die Benachrichtigungsdienste einzustellen, gehen Sie zu **Benachrichtigungen & Protokolle** unter **Monitoring** im BitDefender Menu und gehen dann zu **Einstellungen**.



Benachrichtigungseinstellungen

Mail-Alarme

BitDefender kann den Netzwerkadministrator mit konfigurierbaren Mail-Benachrichtigungen informieren, wenn ein definiertes Ereignis stattfindet. Durch die Aktivierung dieser Funktion erhalten Sie zeitnah wichtige Informationen zum Zustand Ihres Servers. Anhand dieser Informationen können Sie entscheiden, ob Sie über die Management-Konsole weitere Maßnahmen ergreifen müssen.

Beachten Sie
Dieses Modul integriert mit einem SMTP Server. Es arbeitet gut mit einem ESMTP Server, benutzt aber nicht das ESMTP Protokoll weil es auf SMTP implementiert ist.

Um den Mail-Benachrichtigungsdienst zu nutzen, muss wie folgt vorgegangen werden:

1. Wählen Sie **Mail-Benachrichtigungen aktivieren** um den Mail-Benachrichtigungsdienst zu aktivieren.
2. Konfigurieren Sie die SMTP Einstellungen:

- **SMTP-Server** - geben Sie die IP-Adresse des SMTP-Servers ein, der in Ihrem Netzwerk zum Versenden von Nachrichten verwendet wird.
- **Von** - geben Sie die E-Mail-Adresse ein, die im Absenderfeld angezeigt werden soll.

Wichtig
Sie müssen eine für den SMTP-Server gültige E-Mail-Adresse eintragen, da sonst der Fall eintreten kann, dass der Server Nachrichten von einem unbekannten Absender nicht weiterleitet.

3. Wenn der SMTP Server, der benutzt wird um Nachrichten zu versenden, authentifizierung benötigt, wählen Sie **Benutze SMTP Server Authentifizierung** und geben Sie den Benutzernamen und Passwort in die entsprechnenden Felder ein.

Beachten Sie
NTLM Authentifizierung ist nicht unterstützt.

4. Geben sie die Empfänger der E-Mail Beachrichtigungen ein in das **Allgemeine SMTP Empfänger** Text Feld. Um E-Mail Adressen zu entfernen, löschen Sie sie aus dem Text-Feld.

   Um eine E-Mail-Adresse aus einer `txt` Datei zu importieren, klicken Sie auf **Importieren...**, wählen Sie die Datei und klicken Sie auf **Öffnen**.

   Wenn Sie die Liste in eine `txt` Datei exportieren möchten, klicken Sie auf **Exportieren...** und speichern Sie die Datei an dem gewünschten Ort.

Beachten Sie
Die hier festgelegten Empfänger werden bei Eintritt eines Ereignisses, für das dieser Benachrichtigungstyp eingestellt wurde, benachrichtigt. Um verschiedene Empfänger für jedes Ereignis festzulegen, öffnen Sie den Tab Benachrichtigungen und konfigurieren Sie die Ereignisse. Weitere Informationen finden Sie hier: „*Ereignisse konfigurieren*“ (S. 37).

5. Klicken Sie **Speichern**, um die Änderungen zu speichern.

Um diesen Dienst zu deaktivieren, deaktivieren Sie das **Aktiviere E-Mail Benachrichtigung** Feld und klicken Sie **Speichern**.

Net Send-Benachrichtigung

BitDefender kann den Netzwerkadministrator durch das Senden konfigurierbarer Benachrichtigungen über `Net Send` benachrichtigen, wenn ein Ereignis auftritt, für das diese eingestellt wurden.

Beachten Sie

Dieses Modul arbeitet mit dem Befehl Net Send des Windows-Betriebssystem, auf dem das Programm installiert ist. Die Alarmmeldungen beziehen sich auf die Aktivität des Produkts. Damit solche Alarmmeldungen empfangen werden können, muss der Administrator Nachrichten- und Alarmdienst auf dem Server und auf der Client-Arbeitsstation aktivieren. Windows Server 2008 unterstützt keine Net Send Benachrichtigungen.

Um den Net Send Benachrichtigungsdienst zu nutzen, muss wie folgt vorgegangen werden:

1. Wählen Sie **Net Send-Benachrichtigung aktivieren**, um den Net Send-Benachrichtigungsdienst zu aktivieren.
2. Geben Sie die Empfänger der NetSend Benachrichtigungenan, indem Sie ihre Computernamen in das Textfeld **Allgemeine NetSend Empfänger** eingeben. Um Empfänger von der Liste zu entfernen, löschen Sie ihre Computernamen aus dem Textfeld.

   Um Computernamen aus einer `txt` Datei zu importieren, klicken Sie auf **Importieren...**, wählen Sie die Datei aus und klicken Sie dann auf **Öffnen**.

   Wenn Sie die Liste in eine `txt` Datei exportieren möchten, klicken Sie auf **Exportieren...** und speichern Sie die Datei an dem gewünschten Ort.

   Beachten Sie

   Die hier festgelegten Empfänger werden bei Eintritt eines Ereignisses, für das dieser Benachrichtigungstyp eingestellt wurde, benachrichtigt. Um verschiedene Empfänger für jedes Ereignis festzulegen, öffnen Sie den Tab Benachrichtigungen und konfigurieren Sie die Ereignisse. Weitere Informationen finden Sie hier: *„Ereignisse konfigurieren“* (S. 37).

3. Klicken Sie **Speichern**, um die Änderungen zu speichern.

Um diesen Dienst zu deaktivieren, löschen Sie die **Aktiviere NetSend** Auswahl und klicken Sie **Speichern**.

Wichtig

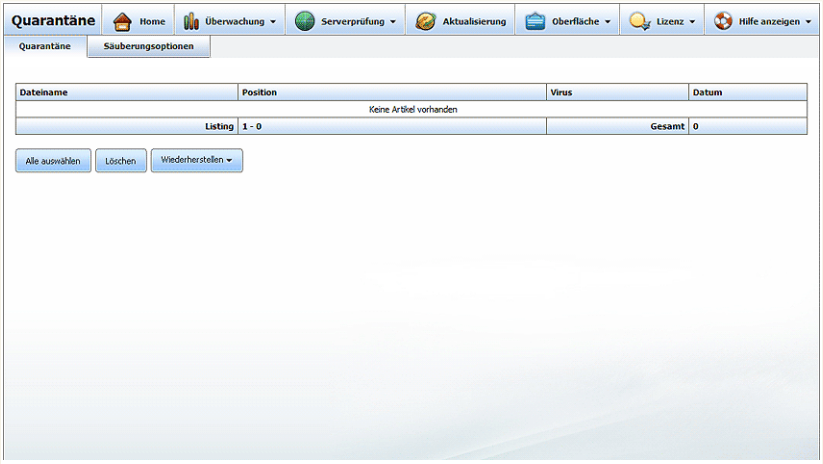
Es ist nicht ratsam, diese Alarmart bei einem Virenausbruch zu verwenden.

7.4. Quarantäne

Mit BitDefender können infizierte oder verdächtige Dateien in einem sicheren Bereich, der Quarantäne, isoliert werden. Indem diese Dateien isoliert werden, kann durch sie keine Infektion ausgelöst werden.

Wichtig
Der Quarantäne-Ordner ist für für die Prüfungen On-Access und On-Demand identisch.

Um die Dateien in Quarantäne zu sehen und sie zu verwalten, gehen Sie zu **Quarantäne** unter **Monitoring** im BitDefender Menu.



Quarantäne

Sie können eine Liste der Dateien in der Quarantäne in der Tabelle aufgelistet sehen. Für jede Datei in Quarantäne, sind die folgenden Informationen verfügbar: der Dateiname, der original Ort, der Virusname und das Datum als sie in Quarantäne kam.

7.4.1. Die Quarantäne verwalten

Verwenden Sie die zur Verfügung stehenden Schaltflächen um die Dateien in der Quarantäne zu verwalten:

- **Alle auswählen** - alle Gegenstände in Quarantäne auswählen
- **Löschen** - löscht die ausgewählten Dateien in Quarantäne
- **Wiederherstellen** - entschlüssele gewählte Dateien in Quarantäne und speichere sie an einem Ort aus der Drop-Down Liste:

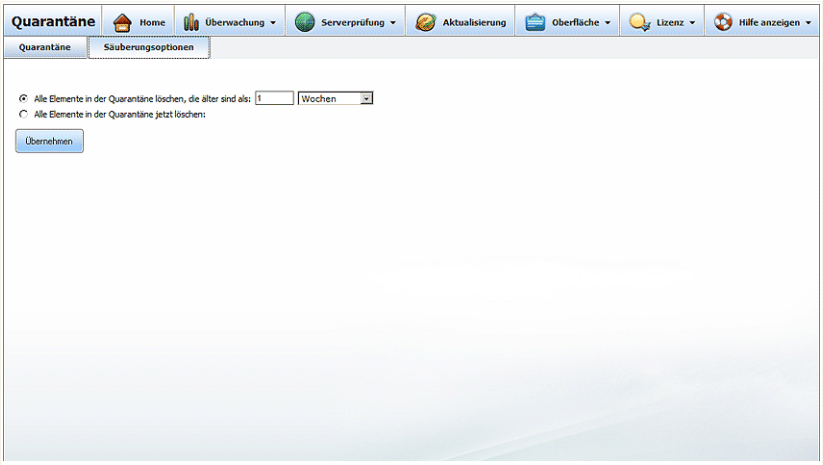
- **Disk Ort** - wählen Sie diese Option, um ausgewählte Dateien auf der HDD wieder herzustellen
- **Web Applikations Ort** - wählen Sie diese Option, um die ausgewählten Dateien an dem Ort der Web Applikation wiederherzustellen
- **Ursprünglicher Ort** - wählen Sie diese Option, um die ausgewählten Dateien an ihrem ursprünglichen Ort wiederherzustellen

Klicke , um einen Ort auszuwählen.

Auf diese Weise können Sie Dateien in Qurantäne öffnen oder ausführen.

7.4.2. Quarantäne löschen

In der Standardeinstellung werden Dateien in der Quarantäne, die älter als eine Woche sind automatisch gelöscht. Um den Zeitraum zu ändern, in dem Dateien in der Quarantäne gespeichert werden, gehen Sie zum **Löschoptionen** Tab auf der **Quarantäne** Seite.



Säuberungsoptionen

Geben Sie die Anzahl der Tage / Wochen / Monate in das entsprechende Feld ein.

Um die Qurantäne manuell zu bereinigen, wählen Sie **Alle Objekte in der Quarantäne jetzt löschen**.

Klicke **Anwenden**, um die Änderungen zu speichern

7.5. Geplante Aufgaben

Geplante Aufgaben bieten eine weitreichende Flexibilität und helfen Ihnen dabei, administrative Sicherheitsaufgaben durchzuführen, ohne dass dabei die Leistung des SharePoint Servers beeinträchtigt wird. Sie können BitDefender so einstellen, dass bestimmte Aufgaben nur ein Mal oder regelmäßig ausgeführt werden. Folgende Aufgaben können eingeplant werden:

- On-Demand Prüfvorgänge.
- Update-Prozesse.
- Aufgaben zur Erstellung eines Berichts.

Um geplante Aufgaben zu erstellen oder zu konfigurieren, gehen Sie zu **Geplante Aufgaben** unter **Monitoring** im BitDefender Menu.

Geplante Aufgaben

Sie können alle eingeplanten Aufgaben aufgelistet in der Tabelle sehen. Für jede Aufgabe werden folgende Informationen zur Verfügung gestellt: Der Name der Aufgabe, der Zeitpunkt der letzten Durchführung, der Zeitpunkt der nächsten eingestellten Durchführung und der Status.

7.5.1. Geplante Aufgaben verwalten

Um geplante Aufgaben zu verwalten, verwenden Sie diese Schaltflächen:

- **Jetzt ausführen** - führt eine ausgewählte geplante Aufgabe durch.
- **Aktivieren/Deaktivieren** - aktiviert/deaktiviert eine oder mehrere ausgewählte Aufgaben.

- **Neue Aufgabe** - startet den Assistenten, der Ihnen beim Erstellen einer neuen zeitgesteuerten Aufgabe hilft.

Beachten Sie
Der Konfigurations-Assistent unterscheidet sich für jede zeitgesteuerte Aufgabe.

- **Aufgabe ansehen** - öffnet das Konfigurationsfenster der ausgewählten Aufgabe, in dem Sie weitere Einstellungen verändern und konfigurieren können.
- **Aufgabe anhalten** - hält die aktuell laufende Aufgabe an.
- **Löschen** - löscht eine oder mehrere ausgewählte Aufgaben. Sie werden aufgefordert, Ihre Auswahl zu bestätigen. Klicken Sie dazu auf **Ja**.

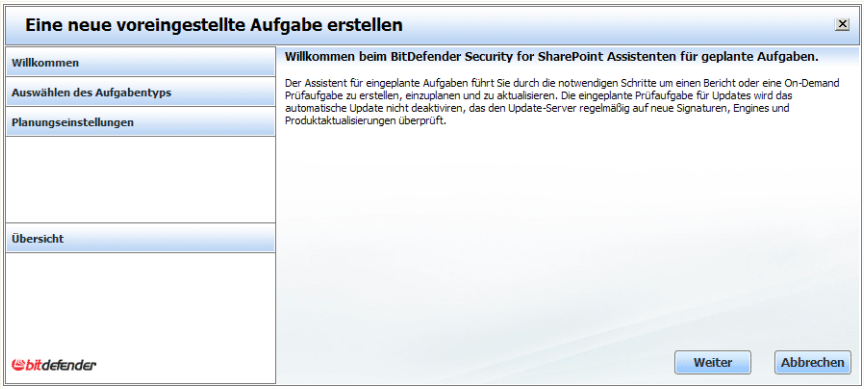
7.5.2. On-Demand Prüfaufgaben

Aufgaben zeitlich einplanen

Sie erstellen eine neue zeitgesteuerte Aufgabe, indem Sie auf **Neue Aufgabe** klicken. Es erscheint ein Konfigurationsassistent, der Sie durch den Prozess der Erstellung einer zeitgesteuerten Aufgabe begleitet.

Befolgen Sie diese Schritte um eine zeitgesteuerte On-Demand Prüfaufgabe einzustellen:

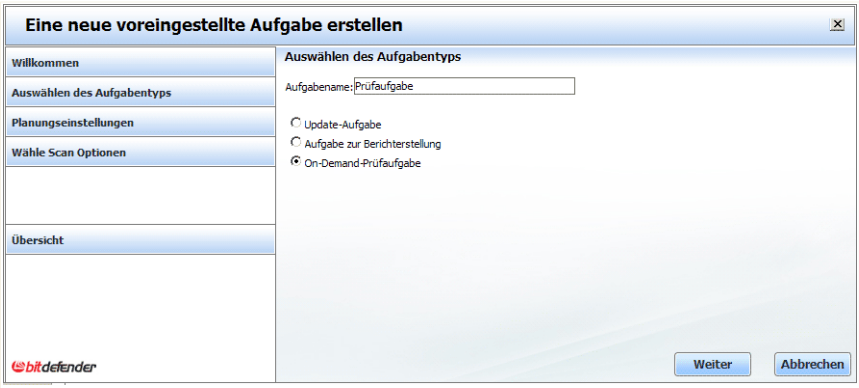
Schritt 1/5 - Willkommen zum Assistenten für geplante Aufgaben


Eine neue voreingestellte Aufgabe erstellen
Willkommen
Auswählen des Aufgabentyps
Planungseinstellungen
Übersicht
bitdefender
Willkommen beim BitDefender Security for SharePoint Assistenten für geplante Aufgaben.
Der Assistent für eingeplante Aufgaben führt Sie durch die notwendigen Schritte um einen Bericht oder eine On-Demand Prüfaufgabe zu erstellen, einzuplanen und zu aktualisieren. Die eingeplante Prüfaufgabe für Updates wird das automatische Update nicht deaktiviren, das den Update-Server regelmäßig auf neue Signaturen, Engines und Produktaktualisierungen überprüft.
Weiter
Abbrechen

Willkommen

Klicken Sie auf **Weiter**.

Schritt 2/5 - Aufgabentyp wählen

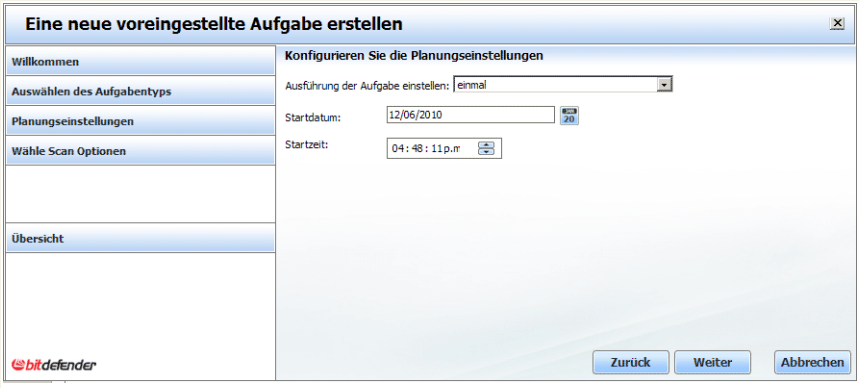


Auswählen des Aufgabentyps

Bitte geben Sie den Namen der Aufgabe an und wählen Sie **On-Demand Prüfaufgabe**.

Klicken Sie auf **Weiter**.

Schritt 3/5 - Planung konfigurieren



Konfigurieren Sie den Aufgabenplan.

Geben Sie den Zeitplan für die Aufgabe an.

Sie müssen eine der folgenden Optionen aus dem Menu wählen:

- **Einmal** - führt das Update nur einmal, zu einem bestimmten Zeitpunkt aus.

  Geben Sie den Zeitpunkt des Starts und des Endes in die Felder **Startdatum/Ende** ein.

- **Periodisch** - führt die Aufgabe periodisch, in bestimmten zeitlichen Abständen (Minuten, Stunden, Tage, Wochen, Monate, Jahre) aus. Der Startpunkt wird mit Datum und Uhrzeit festgelegt.

  Um die nötigen Einstellungen zu konfigurieren, befolgen Sie die folgenden Schritte:

  1. Geben Sie das Startdatum in das Feld **Startdatum** ein.
  2. Wenn Sie möchten, dass die Aufgabe mehrmals bis zu einem bestimmten Datum ausgeführt wird, markieren Sie **Ende** und geben Sie das Datum des Endes in das entsprechende Feld ein.
  3. Geben Sie die Startzeit in das Feld **Startzeit** ein.
  4. Legen Sie die Häufigkeit der Aufgabe fest, indem Sie in das entsprechende Feld die Anzahl der Minuten / Stunden / Tage / Wochen / Monate / Jahre angeben, die zwischen zwei Aufgaben liegen sollen.

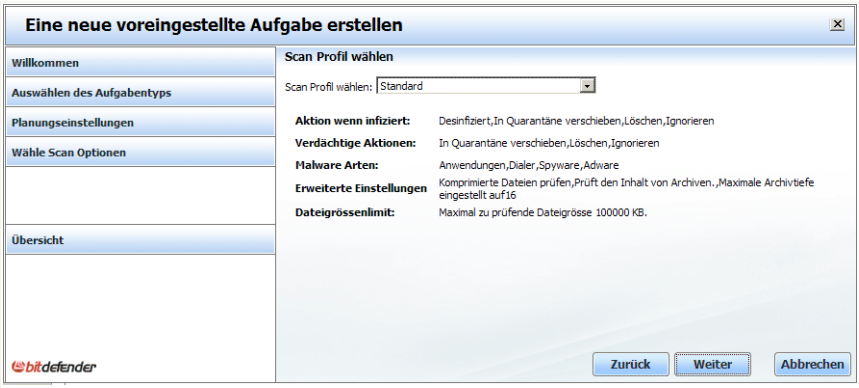
- **Wochentage** - um die Aufgabe mehrmals an bestimmten Wochentagen auszuführen, wobei an einem festgelegten Datum/Uhrzeit begonnen wird.

  Um die nötigen Einstellungen zu konfigurieren, befolgen Sie die folgenden Schritte:

  1. Geben Sie das Startdatum in das Feld **Startdatum** ein.
  2. Wenn Sie möchten, dass die Aufgabe mehrmals bis zu einem bestimmten Datum ausgeführt wird, wählen Sie **Ende** und geben Sie das Enddatum in das entsprechende Feld ein.
  3. Geben Sie die Startzeit in das Feld **Startzeit** ein.
  4. Wählen Sie den Tag oder die Tage an dem/denen die Aufgabe ausgeführt werden soll.

Klicken Sie auf **Weiter**.

Schritt 4/5 - Scan Profil wählen



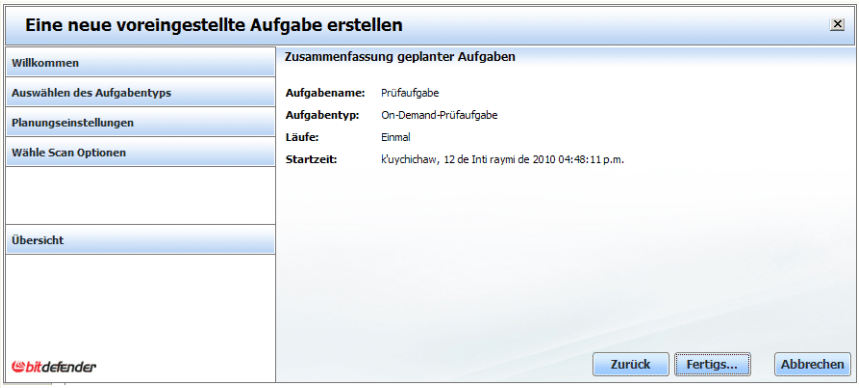
Scan Profil wählen

Sie können eins der folgenden Scan-Profile benutzen:

Scan-Profil	Beschreibung
Hoch	Der SharePoint Server wird nach allen Arten von Malware geprüft. Gepackte Archive werden im Scan eingeschlossen. Die maximale Archivtiefe, die geprüft wird, ist 16. Bitte bedenken Sie, dass nur Dateien unter 100 MB in Grösse geprüft werden.
Niedrig	Ermöglicht einen schnellen Scan des Servers. Dateien werden nach Spyware und Adware untersucht mit einer maximalen Archivtiefe von 8. Nur Dateien unter 50 MB werden geprüft.

Klicken Sie auf **Weiter**.

Schritt 5/5 – Zusammenfassung betrachten



Betrachten Sie die Zusammenfassung

In diesem Fenster können Sie die Aufgabeneinstellungen überprüfen. Sie können alle Änderungen vornehmen, indem Sie zu den vorigen Schritten zurück gehen. Um dies zu tun, klicken Sie **Zurück** um zum vorigen Schritt zurück zu gehen, oder wählen Sie irgendeinen Schritt in der linken Fensterhälfte.

Klicken Sie auf **Beenden**, um die zeitgesteuerte Aufgabe zu speichern.

Beachten Sie
Die Aufgabe wird im Abschnitt Geplante Aufgaben angezeigt.

Eigenschaften konfigurieren

Um eine geplante Aufgabe zu modifizieren, wählen Sie sie und klicken Sie auf **Aufgabe ansehen**.

Der Konfigurationsassistent wird geöffnet. Wählen Sie einen der Schritte in der linken Hälfte des Fensters und klicken Sie **Weiter**, um dem Assistenten Schirtt für Schritt zu folgen.

1. **Willkommen** - die Willkommensseite.
2. **Wähle Aufgabentyp** - ändern Sie den Aufgabennamen.
3. **Planungseinstellungen** - modifizieren Sie die Aufgabenplanung.

   Geben Sie den Zeitplan für die Aufgabe an.

   Sie müssen eine der folgenden Optionen aus dem Menu wählen:

   - **Einmal** - führt das Update nur einmal, zu einem bestimmten Zeitpunkt aus.

     Geben Sie den Zeitpunkt des Starts und des Endes in die Felder **Startdatum/Ende** ein.

- **Periodisch** - führt die Aufgabe periodisch, in bestimmten zeitlichen Abständen (Minuten, Stunden, Tage, Wochen, Monate, Jahre) aus. Der Startpunkt wird mit Datum und Uhrzeit festgelegt.

  Um die nötigen Einstellungen zu konfigurieren, befolgen Sie die folgenden Schritte:

  a. Geben Sie das Startdatum in das Feld **Startdatum** ein.

  b. Wenn Sie möchten, dass die Aufgabe mehrmals bis zu einem bestimmten Datum ausgeführt wird, markieren Sie **Ende** und geben Sie das Datum des Endes in das entsprechende Feld ein.

  c. Geben Sie die Startzeit in das Feld **Startzeit** ein.

  d. Legen Sie die Häufigkeit der Aufgabe fest, indem Sie in das entsprechende Feld die Anzahl der Minuten / Stunden / Tage / Wochen / Monate / Jahre angeben, die zwischen zwei Aufgaben liegen sollen.

- **Wochentage** - um die Aufgabe mehrmals an bestimmten Wochentagen auszuführen, wobei an einem festgelegten Datum/Uhrzeit begonnen wird.

  Um die nötigen Einstellungen zu konfigurieren, befolgen Sie die folgenden Schritte:

  a. Geben Sie das Startdatum in das Feld **Startdatum** ein.

  b. Wenn Sie möchten, dass die Aufgabe mehrmals bis zu einem bestimmten Datum ausgeführt wird, wählen Sie **Ende** und geben Sie das Enddatum in das entsprechende Feld ein.

  c. Geben Sie die Startzeit in das Feld **Startzeit** ein.

  d. Wählen Sie den Tag oder die Tage an dem/denen die Aufgabe ausgeführt werden soll.

4. **Prüfungsoptionen wählen** - Wählen Sie eine der folgenden Prüfungsoptionen:

Scan-Profil	Beschreibung
Hoch	Der SharePoint Server wird nach allen Arten von Malware geprüft. Gepackte Archive werden im Scan eingeschlossen. Die maximale Archivtiefe, die geprüft wird, ist 16. Bitte bedenken Sie, dass nur Dateien unter 100 MB in Grösse geprüft werden.
Niedrig	Ermöglicht einen schnellen Scan des Servers. Dateien werden nach Spyware und Adware untersucht mit einer maximalen Archivtiefe von 8. Nur Dateien unter 50 MB werden geprüft.

5. **Zusammenfassung** - Zeigt die Aufgabeneinstellungen an. Wenn Sie die Aufgabeneigenschaften konfiguriert haben, gehen Sie zu **Zusammenfassung** und klicken Sie **Beenden**, um die Einstellungen zu sichern. Wenn das Konfigurationsfenster schließen möchten ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen**.

7.5.3. Update-Aufgaben

Aufgaben zeitlich einplanen

Sie erstellen eine neue zeitgesteuerte Aufgabe, indem Sie auf **Neue Aufgabe** klicken. Es erscheint ein Konfigurationsassistent, der Sie durch den Prozess der Erstellung einer zeitgesteuerten Aufgabe begleitet.

Beachten Sie
Die zeitgesteuerten Update-Aufgaben haben keinen Einfluss auf das automatische Update.

So richten Sie eine zeitgesteuerte Update-Aufgabe ein:

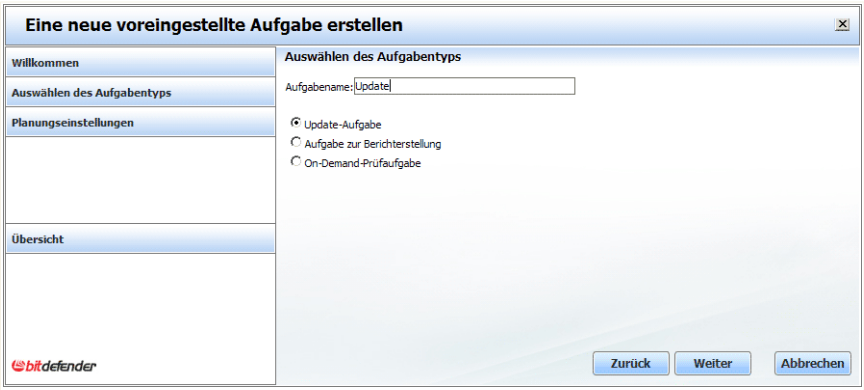
Schritt 1/4 - Willkommen zum Assistenten für zeitgesteuere Aufgaben

Eine neue voreingestellte Aufgabe erstellen
Willkommen
Auswählen des Aufgabentyps
Planungseinstellungen
Übersicht
bitdefender
Willkommen beim BitDefender Security for SharePoint Assistenten für geplante Aufgaben.
Der Assistent für eingeplante Aufgaben führt Sie durch die notwendigen Schritte um einen Bericht oder eine On-Demand Prüfaufgabe zu erstellen, einzuplanen und zu aktualisieren. Die eingeplante Prüfaufgabe für Updates wird das automatische Update nicht deaktiviren, das den Update-Server regelmäßig auf neue Signaturen, Engines und Produktaktualisierungen überprüft.
Weiter
Abbrechen

Willkommen

Klicken Sie auf **Weiter**.

Schritt 2/4 – Aufgabentyp wählen

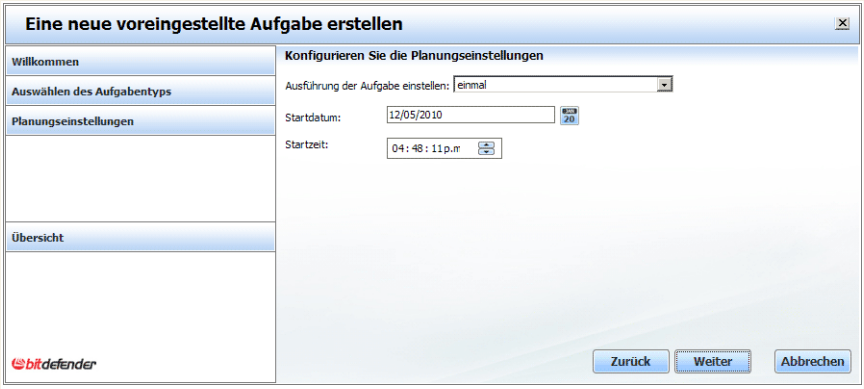


Auswählen des Aufgabentyps

Bitte geben Sie den Namen der Aufgabe an und wählen Sie **Update-Aufgabe**.

Klicken Sie auf **Weiter**.

Schritt 3/4 – Zeitsteuerung konfigurieren



Konfigurieren Sie den Aufgabenplan.

Geben Sie den Zeitplan für die Aufgabe an.

Sie müssen eine der folgenden Optionen aus dem Menu wählen:

- **Einmal** - führt das Update nur einmal, zu einem bestimmten Zeitpunkt aus.

  Geben Sie den Zeitpunkt des Starts und des Endes in die Felder **Startdatum/Ende** ein.

- **Periodisch** - führt die Aufgabe periodisch, in bestimmten zeitlichen Abständen (Minuten, Stunden, Tage, Wochen, Monate, Jahre) aus. Der Startpunkt wird mit Datum und Uhrzeit festgelegt.

  Um die nötigen Einstellungen zu konfigurieren, befolgen Sie die folgenden Schritte:

  1. Geben Sie das Startdatum in das Feld **Startdatum** ein.
  2. Wenn Sie möchten, dass die Aufgabe mehrmals bis zu einem bestimmten Datum ausgeführt wird, markieren Sie **Ende** und geben Sie das Datum des Endes in das entsprechende Feld ein.
  3. Geben Sie die Startzeit in das Feld **Startzeit** ein.
  4. Legen Sie die Häufigkeit der Aufgabe fest, indem Sie in das entsprechende Feld die Anzahl der Minuten / Stunden / Tage / Wochen / Monate / Jahre angeben, die zwischen zwei Aufgaben liegen sollen.

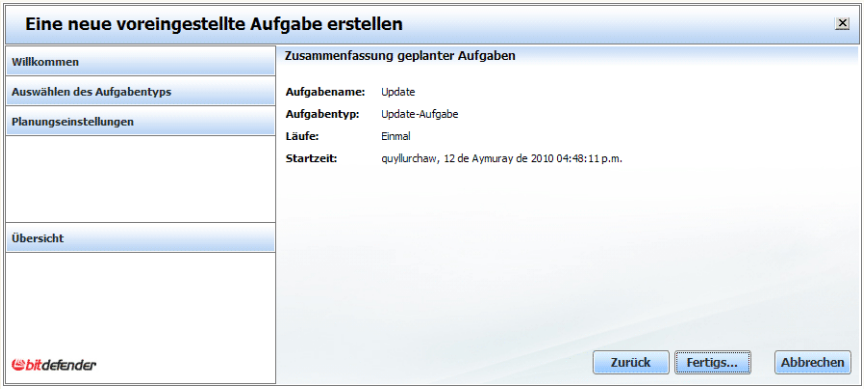
- **Wochentage** - um die Aufgabe mehrmals an bestimmten Wochentagen auszuführen, wobei an einem festgelegten Datum/Uhrzeit begonnen wird.

  Um die nötigen Einstellungen zu konfigurieren, befolgen Sie die folgenden Schritte:

  1. Geben Sie das Startdatum in das Feld **Startdatum** ein.
  2. Wenn Sie möchten, dass die Aufgabe mehrmals bis zu einem bestimmten Datum ausgeführt wird, wählen Sie **Ende** und geben Sie das Enddatum in das entsprechende Feld ein.
  3. Geben Sie die Startzeit in das Feld **Startzeit** ein.
  4. Wählen Sie den Tag oder die Tage an dem/denen die Aufgabe ausgeführt werden soll.

Klicken Sie auf **Weiter**.

Schritt 4/4 – Zusammenfassung



Betrachten Sie die Zusammenfassung

In diesem Fenster können Sie die Aufgabeneinstellungen überprüfen. Sie können alle Änderungen vornehmen, indem Sie zu den vorigen Schritten zurück gehen. Um dies zu tun, klicken Sie **Zurück** um zum vorigen Schritt zurück zu gehen, oder wählen Sie irgendeinen Schritt in der linken Fensterhälfte.

Klicken Sie auf **Beenden**, um die zeitgesteuerte Aufgabe zu speichern.

Beachten Sie
Die neue Aufgabe wird nun im Abschnitt Zeitgesteuerte Aufgaben angezeigt.

Eigenschaften konfigurieren

Um eine geplante Aufgabe zu modifizieren, wählen Sie sie und klicken Sie auf **Aufgabe ansehen**.

Der Konfigurationsassistent wird geöffnet. Wählen Sie einen der Schritte in der linken Hälfte des Fensters und klicken Sie **Weiter**, um dem Assistenten Schirtt für Schritt zu folgen.

1. **Willkommen** - die Willkommensseite.
2. **Wähle Aufgabentyp** - ändern Sie den Aufgabennamen.
3. **Planungseinstellungen** - modifizieren Sie die Aufgabenplanung.

   Geben Sie den Zeitplan für die Aufgabe an.

   Sie müssen eine der folgenden Optionen aus dem Menu wählen:

   - **Einmal** - führt das Update nur einmal, zu einem bestimmten Zeitpunkt aus.

     Geben Sie den Zeitpunkt des Starts und des Endes in die Felder **Startdatum/Ende** ein.

- **Periodisch** - führt die Aufgabe periodisch, in bestimmten zeitlichen Abständen (Minuten, Stunden, Tage, Wochen, Monate, Jahre) aus. Der Startpunkt wird mit Datum und Uhrzeit festgelegt.

  Um die nötigen Einstellungen zu konfigurieren, befolgen Sie die folgenden Schritte:

  a. Geben Sie das Startdatum in das Feld **Startdatum** ein.

  b. Wenn Sie möchten, dass die Aufgabe mehrmals bis zu einem bestimmten Datum ausgeführt wird, markieren Sie **Ende** und geben Sie das Datum des Endes in das entsprechende Feld ein.

  c. Geben Sie die Startzeit in das Feld **Startzeit** ein.

  d. Legen Sie die Häufigkeit der Aufgabe fest, indem Sie in das entsprechende Feld die Anzahl der Minuten / Stunden / Tage / Wochen / Monate / Jahre angeben, die zwischen zwei Aufgaben liegen sollen.

- **Wochentage** - um die Aufgabe mehrmals an bestimmten Wochentagen auszuführen, wobei an einem festgelegten Datum/Uhrzeit begonnen wird.

  Um die nötigen Einstellungen zu konfigurieren, befolgen Sie die folgenden Schritte:

  a. Geben Sie das Startdatum in das Feld **Startdatum** ein.

  b. Wenn Sie möchten, dass die Aufgabe mehrmals bis zu einem bestimmten Datum ausgeführt wird, wählen Sie **Ende** und geben Sie das Enddatum in das entsprechende Feld ein.

  c. Geben Sie die Startzeit in das Feld **Startzeit** ein.

  d. Wählen Sie den Tag oder die Tage an dem/denen die Aufgabe ausgeführt werden soll.

4. **Zusammenfassung** - Zeigt die Aufgabeneinstellungen an. Wenn Sie die Aufgabeneigenschaften konfiguriert haben, gehen Sie zu **Zusammenfassung** und klicken Sie **Beenden**, um die Einstellungen zu sichern. Wenn das Konfigurationsfenster schließen möchten ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen**.

7.5.4. Aufgaben zur Berichterstellung

Aufgaben zeitlich einplanen

Sie erstellen eine neue zeitgesteuerte Aufgabe, indem Sie auf **Neue Aufgabe** klicken. Es erscheint ein Konfigurationsassistent, der Sie durch den Prozess der Erstellung einer zeitgesteuerten Aufgabe begleitet.

So richten Sie eine zeitgesteuerte Aufgabe zur Berichterstellung ein:

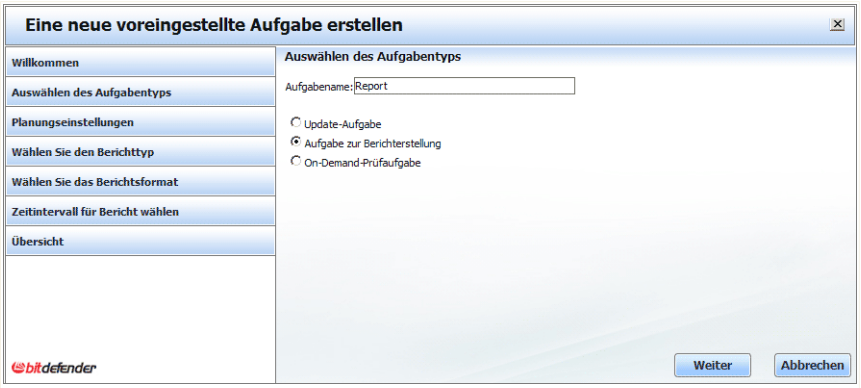
Schritt 1/7 - Willkommen zum Assistenten für zeitgesteuere Aufgaben

Eine neue voreingestellte Aufgabe erstellen
Willkommen
Auswählen des Aufgabentyps
Planungseinstellungen
Übersicht
bitdefender
Willkommen beim BitDefender Security for SharePoint Assistenten für geplante Aufgaben.
Der Assistent für eingeplante Aufgaben führt Sie durch die notwendigen Schritte um einen Bericht oder eine On-Demand Prüfaufgabe zu erstellen, einzuplanen und zu aktualisieren. Die eingeplante Prüfaufgabe für Updates wird das automatische Update nicht deaktiviren, das den Update-Server regelmäßig auf neue Signaturen, Engines und Produktaktualisierungen überprüft.
Weiter
Abbrechen

Willkommen

Klicken Sie auf **Weiter**.

Schritt 2/7 – Aufgabentyp wählen

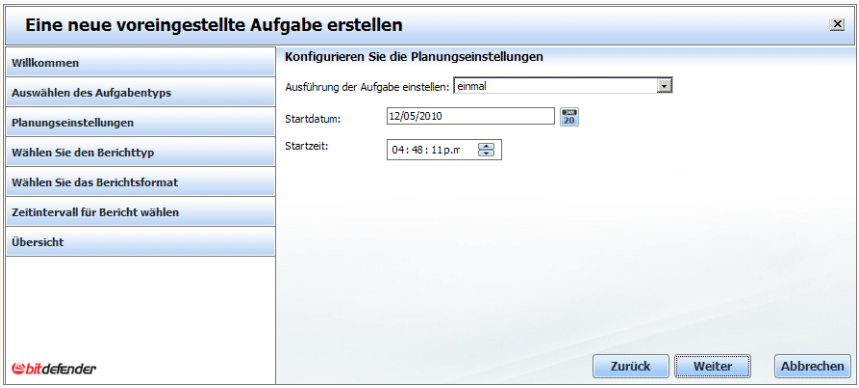


Auswählen des Aufgabentyps

Geben Sie den Namen der Aufgabe an und wählen Sie **Aufgabe zur Berichterstellung**.

Klicken Sie auf **Weiter**.

Schritt 3/7 – Zeitsteuerung konfigurieren



Konfigurieren Sie den Aufgabenplan.

Geben Sie den Zeitplan für die Aufgabe an.

Sie müssen eine der folgenden Optionen aus dem Menu wählen:

- **Einmal** - führt das Update nur einmal, zu einem bestimmten Zeitpunkt aus.

  Geben Sie den Zeitpunkt des Starts und des Endes in die Felder **Startdatum/Ende** ein.

- **Periodisch** - führt die Aufgabe periodisch, in bestimmten zeitlichen Abständen (Minuten, Stunden, Tage, Wochen, Monate, Jahre) aus. Der Startpunkt wird mit Datum und Uhrzeit festgelegt.

  Um die nötigen Einstellungen zu konfigurieren, befolgen Sie die folgenden Schritte:

  1. Geben Sie das Startdatum in das Feld **Startdatum** ein.
  2. Wenn Sie möchten, dass die Aufgabe mehrmals bis zu einem bestimmten Datum ausgeführt wird, markieren Sie **Ende** und geben Sie das Datum des Endes in das entsprechende Feld ein.
  3. Geben Sie die Startzeit in das Feld **Startzeit** ein.
  4. Legen Sie die Häufigkeit der Aufgabe fest, indem Sie in das entsprechende Feld die Anzahl der Minuten / Stunden / Tage / Wochen / Monate / Jahre angeben, die zwischen zwei Aufgaben liegen sollen.

- **Wochentage** - um die Aufgabe mehrmals an bestimmten Wochentagen auszuführen, wobei an einem festgelegten Datum/Uhrzeit begonnen wird.

  Um die nötigen Einstellungen zu konfigurieren, befolgen Sie die folgenden Schritte:

  1. Geben Sie das Startdatum in das Feld **Startdatum** ein.

2. Wenn Sie möchten, dass die Aufgabe mehrmals bis zu einem bestimmten Datum ausgeführt wird, wählen Sie **Ende** und geben Sie das Enddatum in das entsprechende Feld ein.
3. Geben Sie die Startzeit in das Feld **Startzeit** ein.
4. Wählen Sie den Tag oder die Tage an dem/denen die Aufgabe ausgeführt werden soll.

Klicken Sie auf **Weiter**.

Schritt 4/7 – Berichttyp wählen

Wählen Sie den Berichttyp

Wählen Sie eine der zur Verfügung stehenden Berichttypen.

Berichttyp	Beschreibung
Antivirus Gesamt	Bietet umfangreiche Informationen über die Bedrohungen die innerhalb eines bestimmten Zeitraums entdeckt wurden.
Häufigste Viren	Bietet eine Tabelle mit den entdeckten Bedrohungen, die innerhalb eines bestimmten Zeitraums entdeckt wurden, geordnet nach der Anzahl der infizierten Dateien.

Klicken Sie auf **Weiter**.

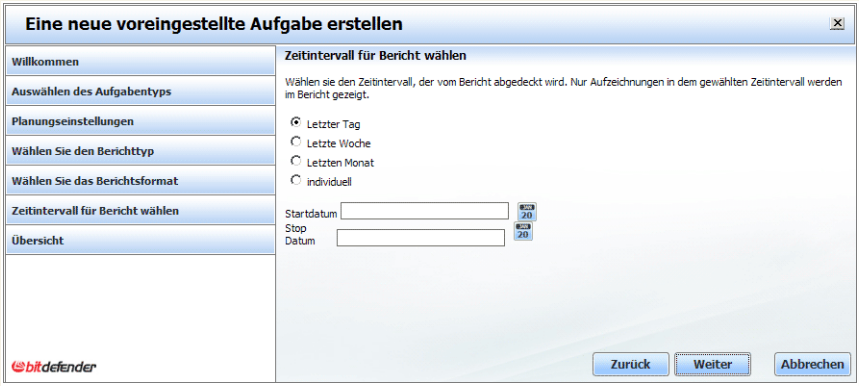
Schritt 5/7 – Berichtsformat wählen

Wählen Sie das Berichtsformat

Wählen Sie das Format der Berichtdatei (**HTML** oder **CSV**).

Klicken Sie auf **Weiter**.

Schritt 6/7 – Zeitintervall einstellen



Wählen Sie den Zeitraum aus

Wählen Sie den im Bericht bedeckten Zeitabstand aus:

- **Letzter Tag**
- **Letzte Woche**
- **Letzter Monat**
- **Benutzerdefiniert**

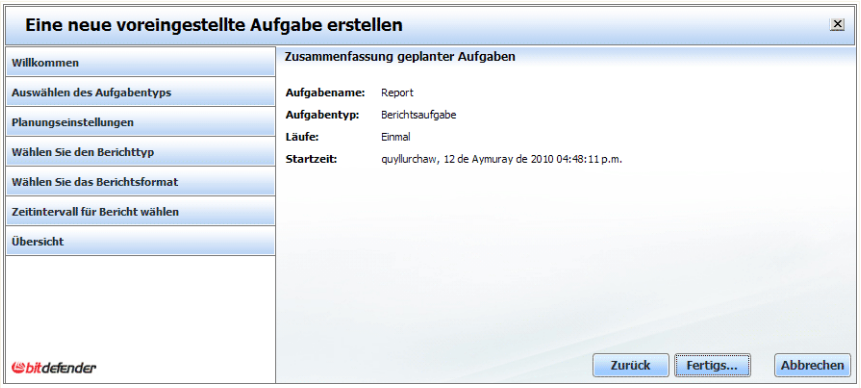
Wenn Sie Information über BitDefender mit einem spezifischen Zeitabstand verbundene Tätigkeit benötigen, wählen Sie **anpassen** und geben Sie das Beginn/Endedatum an. Um Anfangs und Enddaten festzulegen, geben Sie entweder neue Werte in die Datumsfelder oder klicken Sie das Kalender Symbol und wählen Sie Daten vom Kalender.

Beachten Sie
Das Format des Datums ist Monat/Tag/Jahr.

Nur Aufnahmen aus dem festgelegten Zeitraum werden in dem Bericht erscheinen.

Klicken Sie auf **Weiter**.

Schritt 7/7 – Zusammenfassung betrachten



Betrachten Sie die Zusammenfassung

In diesem Fenster können Sie die Aufgabeneinstellungen überprüfen. Sie können alle Änderungen vornehmen, indem Sie zu den vorigen Schritten zurück gehen. Um dies zu tun, klicken Sie **Zurück** um zum vorigen Schritt zurück zu gehen, oder wählen Sie irgendeinen Schritt in der linken Fensterhälfte.

Klicken Sie auf **Beenden**, um die zeitgesteuerte Aufgabe zu speichern.

Beachten Sie
Die neue Aufgabe wird nun im Abschnitt Zeitgesteuerte Aufgaben angezeigt.

Eigenschaften konfigurieren

Um eine geplante Aufgabe zu modifizieren, wählen Sie sie und klicken Sie auf **Aufgabe ansehen**.

Der Konfigurationsassistent wird geöffnet. Wählen Sie einen der Schritte in der linken Hälfte des Fensters und klicken Sie **Weiter**, um dem Assistenten Schirtt für Schritt zu folgen.

1. **Willkommen** - die Willkommensseite.
2. **Wähle Aufgabentyp** - ändern Sie den Aufgabennamen.
3. **Planungseinstellungen** - modifizieren Sie die Aufgabenplanung.

   Geben Sie den Zeitplan für die Aufgabe an.

   Sie müssen eine der folgenden Optionen aus dem Menu wählen:

   - **Einmal** - führt das Update nur einmal, zu einem bestimmten Zeitpunkt aus.

     Geben Sie den Zeitpunkt des Starts und des Endes in die Felder **Startdatum/Ende** ein.

   - **Periodisch** - führt die Aufgabe periodisch, in bestimmten zeitlichen Abständen (Minuten, Stunden, Tage, Wochen, Monate, Jahre) aus. Der Startpunkt wird mit Datum und Uhrzeit festgelegt.

     Um die nötigen Einstellungen zu konfigurieren, befolgen Sie die folgenden Schritte:

     a. Geben Sie das Startdatum in das Feld **Startdatum** ein.

     b. Wenn Sie möchten, dass die Aufgabe mehrmals bis zu einem bestimmten Datum ausgeführt wird, markieren Sie **Ende** und geben Sie das Datum des Endes in das entsprechende Feld ein.

     c. Geben Sie die Startzeit in das Feld **Startzeit** ein.

     d. Legen Sie die Häufigkeit der Aufgabe fest, indem Sie in das entsprechende Feld die Anzahl der Minuten / Stunden / Tage / Wochen / Monate / Jahre angeben, die zwischen zwei Aufgaben liegen sollen.

   - **Wochentage** - um die Aufgabe mehrmals an bestimmten Wochentagen auszuführen, wobei an einem festgelegten Datum/Uhrzeit begonnen wird.

     Um die nötigen Einstellungen zu konfigurieren, befolgen Sie die folgenden Schritte:

     a. Geben Sie das Startdatum in das Feld **Startdatum** ein.

     b. Wenn Sie möchten, dass die Aufgabe mehrmals bis zu einem bestimmten Datum ausgeführt wird, wählen Sie **Ende** und geben Sie das Enddatum in das entsprechende Feld ein.

     c. Geben Sie die Startzeit in das Feld **Startzeit** ein.

     d. Wählen Sie den Tag oder die Tage an dem/denen die Aufgabe ausgeführt werden soll.

4. **BErichtstyp wählen** - wählen Sie einen der folgenden Berichtstypen:

Berichttyp	Beschreibung
Antivirus Gesamt	Bietet umfangreiche Informationen über die Bedrohungen die innerhalb eines bestimmten Zeitraums entdeckt wurden.
Häufigste Viren	Bietet eine Tabelle mit den entdeckten Bedrohungen, die innerhalb eines bestimmten Zeitraums entdeckt wurden, geordnet nach der Anzahl der infizierten Dateien.

5. **Berichtsform wählen** - Wählen Sie das Format der Berichtsdatei: **HTML** oder **CSV**
6. **Wähle Berichtszeit Intervall** - Wählen Sie das Zeitintervall, dass vom Bericht erfasst wird:
   - **Letzter Tag**
   - **Letzte Woche**
   - **Letzter Monat**
   - **Benutzerdefiniert**

   Wenn Sie Information über BitDefender mit einem spezifischen Zeitabstand verbundene Tätigkeit benötigen, wählen Sie **anpassen** und geben Sie das Beginn/Endedatum an. Um Anfangs und Enddaten festzulegen, geben Sie entweder neue Werte in die Datumsfelder oder klicken Sie das Kalender Symbol und wählen Sie Daten vom Kalender.

   Beachten Sie
   Das Format des Datums ist Monat/Tag/Jahr.

   Nur Aufnahmen aus dem festgelegten Zeitraum werden in dem Bericht erscheinen.
7. **Zusammenfassung** - Zeigt die Aufgabeneinstellungen an. Wenn Sie die Aufgabeneigenschaften konfiguriert haben, gehen Sie zu **Zusammenfassung** und klicken Sie **Beenden**, um die Einstellungen zu sichern. Wenn das Konfigurationsfenster schließen möchten ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen**.

8. Serverprüfung

Serverprüfung - ermöglicht die Konfiguration auf welche Weise BitDefender den Server prüft.

BitDefender Security für SharePoint schützt gegen verschiedene Arten von Malware, wie Viren, Spyware, Adware, Rootkits, usw. Das Produkt bietet zwei Schutzebenen:

- Echtzeitprüfung - hindert Benutzer daran infizierte Dateien runter- oder hochzuladen und damit die Infection zu verbreiten. BitDefender prüft Dateien, während sie hoch- oder heruntergeladen werden, entsprechend der aktuellen Sicherheitsstufe. Die Aktionen, die durchgeführt werden sollen, falls infizierte oder verdächtige Dateien entdeckt werden, hängen ebenfalls von der eingestellten Sicherheitsstufe ab.

  Standardmässig ist der Echtzeitschutz auf **Mittel** eingestellt, was eine gute Virenerkennung bei niedrigem Ressourcenverbrauch gewährleistet. BitDefender ist so konfiguriert, dass infizierte Dateien desinfiziert werden und auf nicht desinfizierte und verdächtige der Zugriff verweigert wird. Um Echtzeit Prüfungen einzustellen, gehen Sie zu **Echtzeit Scanner** unter **Server Prüfung** im BitDefender Menu.

  Beachten Sie
  Echtzeit Scanning wird auch Echtzeitschutz genannt - Dateien werden geprüft, wenn Benutzer auf sie zugreifen.

- On-demand Prüfung - erkennt und entfernt Malware die sich bereits auf dem System befindet. Hierbei handelt es sich um eine klassische , durch den Administrator gestartete, Prüfung - Sie wählen das Laufwerk, Ordner oder Datei welche BitDefender prüfen soll, und BitDefender prüft diese auf Anfrage.

  Um Echtzeit Prüfungen einzustellen, gehen Sie zu **Echtzeit Scanner** unter **Server Prüfung** im BitDefender Menu. Sie können verschiedene Prüfmodi durchführen. Wählen Sie den Benutzermodus um die Prüfoptionen und die Locations, die geprüft werden sollen, vollständig zu konfigurieren.

  Sie können On-Demand Prüfaufgaben so einstellen, dass Sie zu einem bestimmten Zeitpunkt und regelmäßig durchgeführt werden. Für weitere Informationen lesen Sie bitte „*Geplante Aufgaben*“ (S. 45).

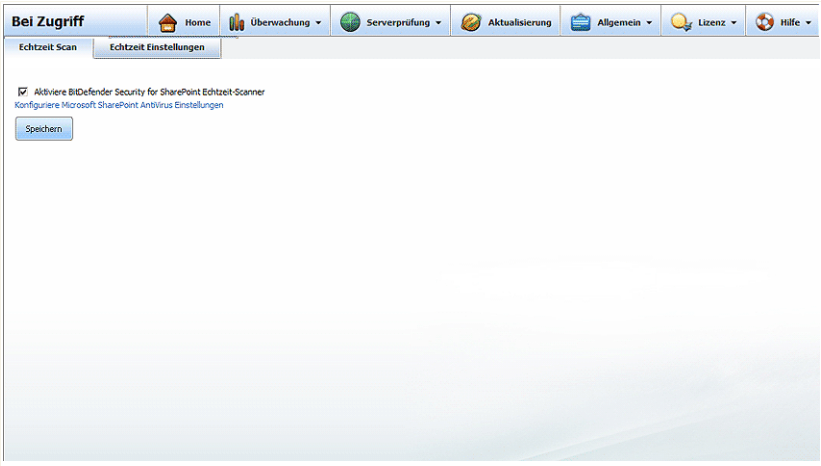
8.1. Echtzeitprüfung

Der Echtzeitschutz schützt den File Server vor neuen Viren, Spyware und Riskware. Es hält Benutzer ebenfalls davon ab, auf infizierte Dateien zuzugreifen oder diese zu kopieren, weshalb einer Virenverbreitung im Netzwerk vorgebeugt wird.

BitDefender prüft Dateien, während sie hoch- oder heruntergeladen werden, entsprechend des aktuellen Scan Profile. Die Aktionen, die durchgeführt werden sollen,

falls infizierte oder verdächtige Dateien entdeckt werden, hängen ebenfalls von der eingestellten Sicherheitsstufe ab.

Um Echtzeit Prüfungen einzustellen, gehen Sie zu **Echtzeit Scanner** unter **Server Prüfung** im BitDefender Menu.



On-Access-Scanner

Die Echtzeitprüfung ist standardmässig aktiviert. Wenn Sie es deaktivieren wollen, gehen Sie zu **Aktiviere BitDefender Security für SharePoint Echtzeit Scanner** und klicken Sie **Speichern**.

Wichtig
Lassen Sie den Echtzeitschutz aktiviert, um den SharePoint Server und die Workstations vor Viren, Spyware und anderer Malware zu schützen.

8.1.1. Konfiguriere Microsoft SharePoint AntiVirus Einstellungen

MicroSoft Office SharePoint Server 2007 erlaubt es Ihnen von der Antiviruis Seite allgemeine Einstellungen für den Virus Scan vorzunehmen.

Sie können auf diese Seite durch klicken auf **Konfiguriere Microsoft SharePoint Antivirus Einstellungen** auf der BitDefender Echtzeitprüfungsseite.

Die folgenden Einstellungen können konfiguriert werden:

- **Antivirus Einstellungen** - wählen Sie die Optionen, die Sie aktivieren wollen:
  - Dokumente beim hochladen prüfen
  - Dokumente beim herunterladen prüfen.
  - Erlaube Benutzern infizierte Dokumente herunterzuladen

- Versuche infizierte Dokumente zu säubern

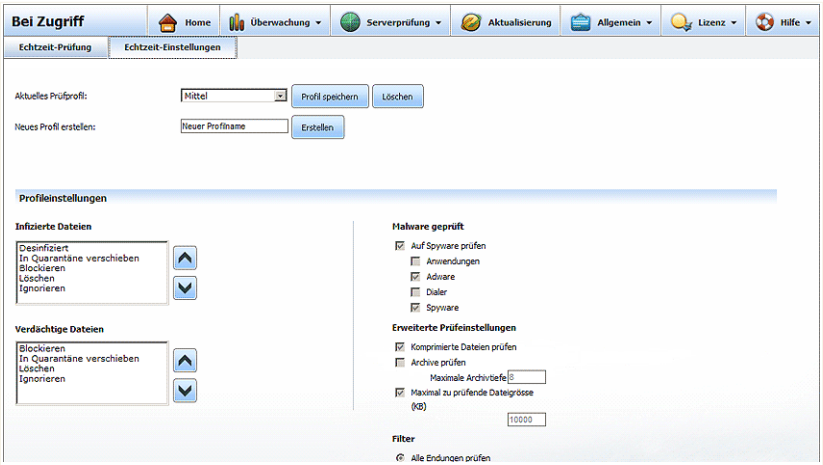
- **Antivirus Time Out** - geben Sie an wie lange der Virus Scanner laufen sollte, vor dem Time-Out.
- **Antivirus Threads** - geben Sie die Anzahl der ausführbaren Threads auf dem Server an, die der Virus Scanner benutzen kann.

Klicke **OK**, um die gewählten Einstellungen zu sichern.

Beachten Sie
Um mehr Informationen über die Konfiguration von Microsoft Office SharePoint Server 2007 Antivirus Einstellungen zu erhalten, beziehen Sie sich bitte auf die Produktdokumentation.

8.1.2. Prüfungsprofile

Um diesen Abschnitt zu öffnen, gehen Sie zu **Echzeit Scanner** unter **Server Scan** im BitDefender Menu und wählen Sie **Echtzeit Einstellung**.



Prüfungsprofile

Hier können Sie die Echtzeit Antivirus Profile konfigurieren.

Profile Verwalten

Alle existierenden Profile erscheinen in der **Aktuelle Prüfprofile** Liste. Wählen Sie ein Profil aus der Liste und sie können die detaillierten Einstellungen betrachten im Abschnitt **Profileinstellungen**

Die Aktionen die für infizierte oder verdächtige Dateien durchgeführt werden sollen, sind kofigurierbar für jedes Scan-Profil. Für weitere Informationen zu den standard Profilen, beziehen Sie sich bitte auf „*Konfiguriere Standard Scanprofile*“ (S. 67).

Wenn Sie die Prüfeinstellungen ebenfalls konfigurieren wollen, müssen Sie individuelle Profile erstellen. Für mehr Informationen zur Erstellung von individuellen Profilen, gehen Sie zu „*Individuelle Scan Profile erstellen*“ (S. 69)

Um die Prüfprofile zu verwalten, benutzen Sie die verfügbaren Buttons:

- Aktivieren Sie das Echtzeit Prüfungsprofil, indem Sie es aus der Liste auswählen und clicken Sie auf **Änderungen Speichern**.
- Aktivieren Sie das Echtzeit Prüfungsprofil, indem Sie es aus der Liste auswählen und clicken Sie auf **Änderungen Speichern**.
- Löschen Sie ein Profil, indem Sie es von der Liste auswählen und klicken Sie **Löschen**.

Beachten Sie
Default profiles can not be deleted.

- Erstellen Sie ein neues Prüfprofil, indem Sie einen Namen in das Feld **Erstelle ein neues Profil Feld** und klicken Sie **Erstellen**.

Konfiguriere Standard Scanprofile

Prüfungsprofile erlauben Ihnen die einfache Konfiguration der Echtzeitprüfung. Sie können eine der standard Prüfungsprofile verwenden oder ein individuelles Profil erstellen.

Die standard Prüfungsprofile werden in der folgenden Tabelle beschrieben:

Prüfungsprofile	Beschreibung
Hoch	Gewährleistet hohe Sicherheit. Mittlere Belastung der Ressourcen. • Alle herunter- und hochgeladenen Dateien, unabhängig ihrer Dateierweiterung und Grösse, werden geprüft. • Dateien werden für alle Arten von Malware (Viren, Trojaner, Spyware, Adware, Riskware, Dialer, usw.) • BitDefender überprüft den Inhalt von Archiven. • Die Standardaktion für infizierte Dateien lautet **Desinfizieren**. Wenn die Desinfektion fehlschlägt, wird die infizierte Datei in die Quarantäne verschoben. • Die Standardeinstellung für verdächtige Dateien lautet **Zugriff verweigern**.
Mittel	Gewährleistet Standard Sicherheit. Belastung der Ressourcen ist gering. • Nur die Dateien, die nicht 10 MB überschreiten werden geprüft. • Dateien werden nur auf Viren, Adware und Spyware geprüft.

Prüfungsprofile	Beschreibung
	• BitDefender prüft nicht den Inhalt von Archiven. • Die Standardaktion für infizierte Dateien lautet **Desinfizieren**. Wenn die Desinfektion fehlschlägt, wird die infizierte Datei in die Quarantäne verschoben. • Die Standardeinstellung für verdächtige Dateien lautet **Zugriff verweigern**.
Niedrig	Deckt einfache Anforderungen ab. Geringe Belastung der Ressourcen. • Nur Dateien auf die zugegriffen wird und die eine Größe von 5 MB nicht überschreiten werden geprüft. • Dateien werden nur auf Viren, Adware und Spyware geprüft. • BitDefender prüft nicht den Inhalt von Archiven. • Die Standardaktion für infizierte Dateien lautet **Desinfizieren**. Wenn die Desinfektion fehlschlägt, wird das herunterladen oder hochladen solcher Dateien nicht zugelassen. • Die Standardeinstellung für verdächtige Dateien lautet **Zugriff verweigern**.

Jedes standard Scan Profil erlaubt die Konfiguration von Aktionen, die bei infizierten oder verdächtigen Dateien durchgeführt werden sollen. Wenn eine infizierte Datei entdeckt wird, so wird die erste Aktion auf der entsprechenden Liste angewendet. Wenn diese Aktion fehlschlägt, wird die nächste Aktion angewendet, usw.

Sie können die Reihenfolge, in der die Aktionen angewendet werden verändern. Wählen Sie eine Aktion und klicken Sie auf oder um sie in der Liste nach oben oder nach unten zu verschieben.

Aktionen für infizierte Dateien. Folgende Aktionen stehen für infizierte Dateien zur Verfügung:

Aktion	Beschreibung
Desinfizieren	Den Malware-Kode aus den infizierten Dateien entfernen. Das Desinfizieren kann in manchen Fällen fehlschlagen, beispielsweise wenn die infizierte Datei sich in speziellen Mail-Archiven befindet.
Verweigern	Hoch- oder Runterladen von infizierten Dateien durch Benutzer verweigern.
In Quarantäne verschieben	Infizierte Dateien von Ihrer ursprünglichen Position in den Quarantäne-Ordner verschieben. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko?

Aktion	Beschreibung
Löschen	Infizierte Dateien direkt und ohne Warnung vom Server entfernen.
Ignorieren	Die infizierten Dateien einfach ignorieren. ***Warnung*** Nicht als erste Aktion in der Liste **Ignorieren** einstellen. Dies zu tun erlaubt Benutzern alle infizierten Dateien hoch und runter zu laden.

Aktionen für verdächtige Dateien. Folgende Aktionen stehen für verdächtige Dateien zur Verfügung:

Aktion	Beschreibung
Verweigern	Hoch- oder Runterladen von infizierten Dateien durch Benutzer verweigern.
In Quarantäne verschieben	Verdächtige Dateien von der ursprünglichen Position in den Quarantäne-Ordner verschieben. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko?
Löschen	Verdächtige Dateien direkt und ohne Warnung vom Server entfernen.
Ignorieren	Die infizierten Dateien einfach ignorieren. Sie sollten diese Aktion nicht als erste Aktion in der Liste auswählen, außer wenn sie ausdrücklich wünschen, dass ALLE verdächtigen Dateien hoch- und heruntergeladen werden. Dies stellt ein hohes Sicherheitsrisiko dar, denn einige dieser Dateien können Schädlinge beinhalten.

Klicken Sie **Änderungen Speichern**, um die Änderungen anzuwenden.

Individuelle Scan Profile erstellen

Stellen Sie fest, dass die mit den standard Scan-Profilen nicht zufrieden sind, können Sie individuelle Profile erstellen. Zur Erstellung eines individuellen Profils, folgen Sie diesen Schritten.

1. Wählen Sie ein Scan-Profil aus der Liste. Die Einstellungen des gewählten Profils wird die Standardeinstellung des neuen Profils sein.
2. Geben Sie den Namen des Profils in das Feld **Neues Profil erstellen** ein.
3. Klicken Sie auf **Erstellen**.

Das neu erstellte Profil erscheint in der Liste **Aktuelles Scan-Profil**. Um zu lernen, wie man individuelle Profile erstellt, gehen Sie bitte zu *„Konfiguriere individuelle Scan-Profile“ (S. 70)*.

Konfiguriere individuelle Scan-Profile

Um die Einstellungen eines individuellen Scan Profils zu konfigurieren, müssen Sie es erst aus der LIste auswählen. Die folgenden Optionen können im Bereich **Profileinstellungen** konfiguriert werden:

Einstellungen	Beschreibung
Aktionen	Konfigurieren Sie die durchzuführenden Aktionen für durch BitDefender entdeckte Dateien die infiziert oder verdächtig sind.
Malware geprüft	Wählen Sie die Arten von Malware aus, nach denen BitDefender Suchen soll.
Erweiterte Scan Einstellungen	BitDefender Konfigurieren gepackte Dateien, Archive oder Dateien, die einen voreingestellten Wert überschreiten, zu prüfen.
Filter	Konfigurieren Sie BitDefender nur Dateien mit bestimmten Endungen zu prüfen.

Aktionen konfigurieren

Sie können verschiedene Aktionen für verdächtige und infizierte Dateien festlegen. Es gibt eine Aktionsliste die für jede Kategorie entdeckter Dateien angewendet werden kann (infiziert oder verdächtig). Wenn eine infizierte Datei entdeckt wird, so wird die erste Aktion auf der entsprechenden Liste angewendet. Wenn diese Aktion fehlschlägt, wird die nächste Aktion angewendet, usw.

Sie können die Reihenfolge, in der die Aktionen angewendet werden verändern. Wählen Sie eine Aktion und klicken Sie auf oder um sie in der Liste nach oben oder nach unten zu verschieben.

Aktionen für infizierte Dateien. Folgende Aktionen stehen für infizierte Dateien zur Verfügung:

Aktion	Beschreibung
Desinfizieren	Den Malware-Kode aus den infizierten Dateien entfernen. Das Desinfizieren kann in manchen Fällen fehlschlagen, beispielsweise wenn die infizierte Datei sich in speziellen Mail-Archiven befindet.
Verweigern	Hoch- oder Runterladen von infizierten Dateien durch Benutzer verweigern.

Aktion	Beschreibung
In Quarantäne verschieben	Infizierte Dateien von Ihrer ursprünglichen Position in den Quarantäne-Ordner verschieben. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko?
Löschen	Infizierte Dateien direkt und ohne Warnung vom Server entfernen.
Ignorieren	Die infizierten Dateien einfach ignorieren. ***Warnung*** Nicht als erste Aktion in der Liste **Ignorieren** einstellen. Dies zu tun erlaubt Benutzern alle infizierten Dateien hoch und runter zu laden.

Aktionen für verdächtige Dateien. Folgende Aktionen stehen für verdächtige Dateien zur Verfügung:

Aktion	Beschreibung
Verweigern	Hoch- oder Runterladen von infizierten Dateien durch Benutzer verweigern.
In Quarantäne verschieben	Verdächtige Dateien von der ursprünglichen Position in den Quarantäne-Ordner verschieben. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko?
Löschen	Verdächtige Dateien direkt und ohne Warnung vom Server entfernen.
Ignorieren	Die infizierten Dateien einfach ignorieren. Sie sollten diese Aktion nicht als erste Aktion in der Liste auswählen, außer wenn sie ausdrücklich wünschen, dass ALLE verdächtigen Dateien hoch- und heruntergeladen werden. Dies stellt ein hohes Sicherheitsrisiko dar, denn einige dieser Dateien können Schädlinge beinhalten.

Malwareprüfung konfigurieren

BitDefender kann Dateien nicht nur nach Viren scannen, sondern auch nach Riskware Bedrohungen. Um BitDefender für das Scannen nach Rickware zu konfigurieren, gehen Sie zum Bereich **Geprüfte Malwared**, wählen Sie erst **Prüfe nach Riskware** und wählen Sie dann nach welchen Arten von Riskware BitDefender wählen soll.

- Anwendungen
- Adware
- Dialer

- Spyware

Fortgeschrittene Prüfeinstellungen konfigurieren.

Die folgenden fortgeschrittenen Einstellungen können im Bereich **Fortgescrittene Scan-Einstellungeb** konfiguriert werden:

- **Gepackte Dateien Scannen** - wählen Sie diese Option, um in gepackten Dateien zu scannen.
- **Scanne in Archiven** - wählen Sie diese Option, um in Archiven zu scannen. Geben sie die maximal zu scanende Archivtiefe an im Feld **Max Archivtiefeh**.
- **MAximal zu scanende Architiefe (KB)** - wählen Sie diese Option, um die maximale Archivtiefe anzugeben, die BitDefender Scannen wird. Geben Sie die Grösse in dem entsprechenden Feld ein.

Filter konfigurieren

Bestimmte Dateisorten sind anfälliger auf Viren als andere. So ist zum Beispiel das Risiko beim Ausführen einer `.exe` Datei höher, als beim Öffnen einer `.txt` oder einer `.gif` Datei.

Um festzulegen welche Dateisorten geprüft werden sollen, wählen Sie eine der folgenden Optionen im Bereich **Filter** :

Optionen	Beschreibung
Alle Endungen prüfen	Alle Dateien auf die zugegriffen wird werden unabhängig von ihrem Typ geprüft.
Nur Anwendungsdateien prüfen	Nur Anwendungsdateien werden geprüft. Diese Kategorie ist auf Dateien mit den folgenden Erweiterungen beschränkt: `386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct;`

Optionen	Beschreibung
	shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp Viren werden normalerweise über Anwendungsdateien übertragen. Deswegen sollten diese Dateiarten immer bei Zugriff geprüft werden.
Benutzerdefinierte Endungen prüfen	Nur Dateien mit den festgelegten Endungen werden geprüft. Sie müssen in das Editierfeld die Dateieendungen eingeben, die von BitDefender geprüft werden sollen, wobei diese mit Strichpunkten (";") zu trennen sind.
Alle bis auf die folgenden Endungen prüfen	Die Dateien mit den festgelegten Endungen werden NICHT geprüft. Sie müssen in das Editierfeld die Dateieendungen eingeben, die NICHT von BitDefender geprüft werden sollen, wobei diese mit Strichpunkten (";") zu trennen sind. Sie sollten Dateiearten, die bekannt für Vren sind nicht von der Prüfung ausschließen, wie beispielsweise `.exe`, `.doc`, `.ppt`, `.xls`, `.rtf`, `.pif`, `.bat` und Andere.

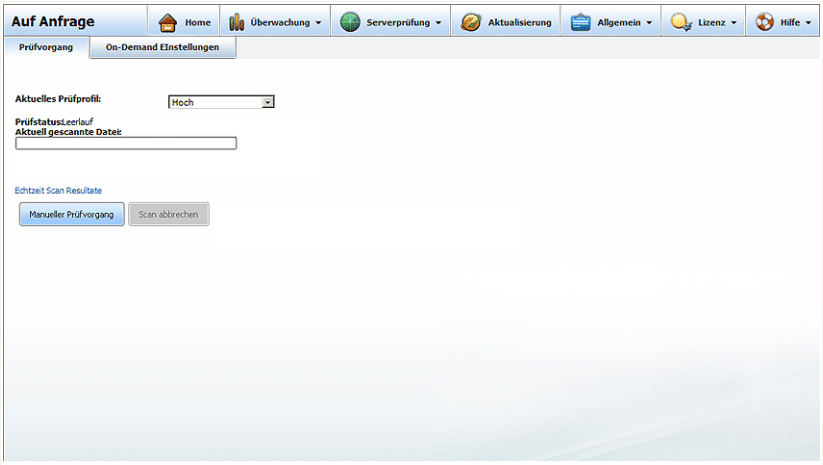
Nach Abschluss der Konfiguration des individuellen Profils, klicken Sie **Änderungen speichern**, um die Einstellungen zu speichern.

8.2. Prüfvorgang

Die On-Demand-Prüfung bietet eine weitere Schutzebene für den SharePoint Server. Sie sollten den Server in regelmäßigen Abständen prüfen, um sicherzustellen, dass er frei von Schad-Software ist. Es wird empfohlen jede Woche eine umfangreiche Systemprüfung durchzuführen.

Wichtig
Gleich nach der Installation des BitDefender Security for SharePoint Servers, führen Sie eine On-Demand Prüfung um irgendwelche Infektionen, die sich bereits auf Ihrem Computer befinden, zu entdecken bsw. zu löschen.

Um Echtzeit Prüfungen einzustellen, gehen Sie zu **Echtzeit Scanner** unter **Server Prüfung** im BitDefender Menu.



On-Demand-Scanner

Die On-Demand-Prüfung basiert auf die Scan-Profile. Scan-Profil Spezifikationen:

- die zu prüfenden Locations (Laufwerke, Ordner, Dateien).
- die Prüfeinstellungen.
- die vom Prüfvorgang ausgeschlossenen Objekte.
- die durchzuführenden Aktionen für entdeckte Dateien die infiziert oder verdächtig sind.

Weitere Informationen erhalten Sie unter *„Prüfungsprofile“* (S. 75).

8.2.1. Dateien und Ordner prüfen

Hier einige Tipps zur On-Demand-Prüfung:

- Vermeiden Sie die Prüfung des Servers, wenn der Server ausgelastet ist, vor allem im Falle einer vollständigen Prüfung. Es wird empfohlen Prüfungen durchzuführen wenn der Server vollkommen oder fast unausgelastet ist. Beispielsweise sollten Sie tiefgehende Systemprüfungen Nachts oder am Wochenende durchführen (planen).
- Bevor Sie die Prüfung starten sollten Sie BitDefender aktualisieren damit das Programm die aktuellste Malware entdecken kann. Um BitDefender unverzüglich zu aktualisieren, befolgen Sie die folgenden Schritte:
  1. Im BitDefender Menu klicken Sie **Update**.
  2. Auf dem **Update** Tab, klicken Sie **Jetzt Updaten**.

Wenn Sie eine voreingestellte Prüfaufgabe für eine regelmäßige Ausführung eingestellt haben, so sollten Sie ebenfalls eine voreingestellte Update-Aufgabe konfigurieren, die wenige Minuten vor der Prüfung ausgeführt wird.

Wichtig
Wenn Sie das automatische Update deaktiviert haben oder die Häufigkeit von Updates niedrig ist, so ist die Aktualisierung von BitDefender vor der Prüfung ein MUSS.

- Führen Sie einmal pro Woche eine tiefgehende Systemprüfung durch, um sicherzugehen, dass sich keine Malware auf Ihrem System befindet. Stellen Sie zu diesem Zweck in geeigneter Weise eine wöchentliche On-Demand-Prüfaufgabe ein. Für weitere Informationen lesen Sie bitte „*Geplante Aufgaben*“ (S. 45).

Um Dateien und Ordner auf Malware zu prüfen, befolgen Sie folgende Schritte:

1. Gehen Sie zu **On-demand scan**.
2. Scan Profil wählen.
3. Klicken Sie auf **Prüfen**, um die Prüfung zu starten.

Während der Prüfung werden die Informationen über den Fortschritt angezeigt:

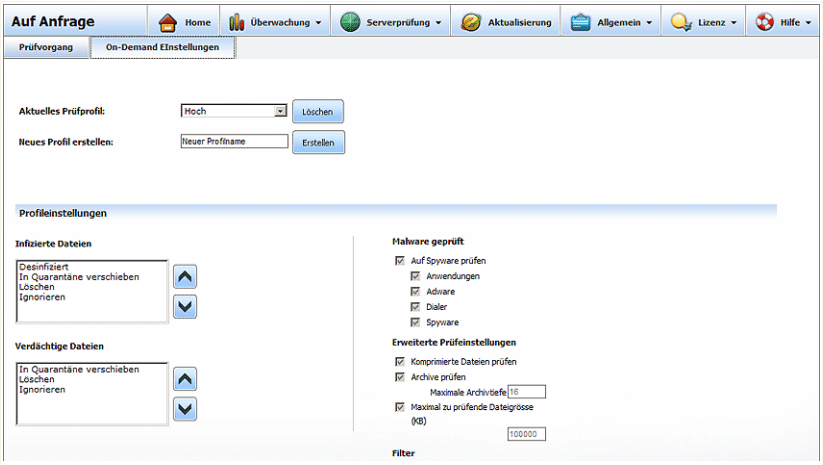
- **Scan Status** Zeigt die Aktivität des Scanners an
- **Aktuell geprüfte Datei** zeigt den Namen und den Pfad der Datei an, die aktuell gescannt wird. Die Fortschrittsanzeige zeigt den Fortschritt jeder Datei während des Scans an.

Sie können die Prüfung jederzeit anhalten, indem Sie **Abbrechen**klicken.

Ein detaillierter Prüfbericht wird jedes Mal erstellt, wenn Sie eine On-Demand-Prüfung durchführen. Um die Prüfungsberichte anzuschauen, klicken Sie **Echtzeit-Prüfungs Ergebnisse** und gehen dann zu Berichte.

8.2.2. Prüfungsprofile

Um diesen Abschnitt zu öffnen, gehen Sie zu **Echzeit Scanner** unter **Server Scan** im BitDefender Menu und wählen Sie **Echtzeit Einstellung**.



Echtzeit Scan Profile

Hier können Sie die Echtzeit Antivirus Profile konfigurieren.

Profile Verwalten

Alle existierenden Profile erscheinen in der **Aktuelle Prüfprofile** Liste. Wählen Sie ein Profil aus der Liste und sie können die detaillierten Einstellungen betrachten im Abschnitt **Profileinstellungen**

Die Aktionen die für infizierte oder verdächtige Dateien durchgeführt werden sollen, sind kofigurierbar für jedes Scan-Profil. „*Konfiguriere Standard Scanprofile*“ (S. 77).

Wenn Sie die Prüfeinstellungen ebenfalls konfigurieren wollen, müssen Sie individuelle Profile erstellen. Für mehr Informationen zur Erstellung von individuellen Profilen, gehen Sie zu „*Individuelle Scan Profile erstellen*“ (S. 78).

Um die Prüfprofile zu verwalten, benutzen Sie die verfügbaren Buttons:

- Aktivieren Sie das Echtzeit Prüfungsprofil, indem Sie es aus der Liste auswählen und clicken Sie auf **Änderungen Speichern**.
- Löschen Sie ein Profil, indem Sie es von der Liste auswählen und klicken Sie **Löschen**.

Beachten Sie
Default scanning profiles can not be deleted.

- Erstellen Sie ein neues Prüfprofil, indem Sie einen Namen in das Feld **Erstelle ein neues Profil Feld** und klicken Sie **Erstellen**.
- Scan Ort eines standard Profils ansehen, oder wählen sie den Scan Ort eines individuellen Profils, indem Sie auf **Scan Ort auswählen** klicken.

Konfiguriere Standard Scanprofile

Prüfungsprofile erlauben Ihnen die einfache Konfiguration der Echtzeitprüfung. Sie können eine der standard Prüfungsprofile verwenden oder ein individuelles Profil erstellen.

Die standard Prüfungsprofile werden in der folgenden Tabelle beschrieben:

Prüfungsprofile	Beschreibung
Hoch	Erlaubt die Durchführung eines umfassenden Scans der Zentralen Administration und aller Orte. Durch die voreingestellten Prüfeinstellungen wird die höchste Effizienz bei der Virenentdeckung gewährleistet. Standardmäßig ist BitDefender so konfiguriert, dass folgende Aktionen durchgeführt werden: ● Infizierte Dateien **Desinfizieren**. Wenn die Desinfektion fehlschlägt, wird die infizierte Datei in die Quarantäne verschoben. ● **Verdächtige Datei in Quarantäne verschieben**.
Niedrig	Erlaubt einen schnellen Scan aller Orte anhand einer vordefinierten Konfiguration der Scan Einstellungen. Nur Dateien, die nicht grösser als 5 MB sind, werden gescannt. Standardmäßig ist BitDefender so konfiguriert, dass folgende Aktionen durchgeführt werden: ● Infizierte Dateien **Desinfizieren**. Wenn die Desinfektion fehlschlägt, wird die infizierte Datei in die Quarantäne verschoben. ● **Verdächtige Datei in Quarantäne verschieben**.

Jedes standard Scan Profil erlaubt die Konfiguration von Aktionen, die bei infizierten oder verdächtigen Dateien durchgeführt werden sollen. Wenn eine infizierte Datei entdeckt wird, so wird die erste Aktion auf der entsprechenden Liste angewendet. Wenn diese Aktion fehlschlägt, wird die nächste Aktion angewendet, usw.

Sie können die Reihenfolge, in der die Aktionen angewendet werden verändern. Wählen Sie eine Aktion und klicken Sie auf oder um sie in der Liste nach oben oder nach unten zu verschieben.

Aktionen für infizierte Dateien. Folgende Aktionen stehen für infizierte Dateien zur Verfügung:

Aktion	Beschreibung
Desinfizieren	Den Malware-Kode aus den infizierten Dateien entfernen. Das Desinfizieren kann in manchen Fällen fehlschlagen,

Aktion	Beschreibung
	beispielsweise wenn die infizierte Datei sich in speziellen Mail-Archiven befindet.
In Quarantäne verschieben	Infizierte Dateien von Ihrer ursprünglichen Position in den Quarantäne-Ordner verschieben. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko?
Löschen	Infizierte Dateien direkt und ohne Warnung vom Server entfernen.
Ignorieren	Die infizierten Dateien einfach ignorieren. ***Warnung*** Nicht als erste Aktion in der Liste **Ignorieren** einstellen. Dies zu tun erlaubt Benutzern alle infizierten Dateien hoch und runter zu laden.

Aktionen für verdächtige Dateien. Folgende Aktionen stehen für verdächtige Dateien zur Verfügung:

Aktion	Beschreibung
In Quarantäne verschieben	Verdächtige Dateien von der ursprünglichen Position in den Quarantäne-Ordner verschieben. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko?
Löschen	Verdächtige Dateien direkt und ohne Warnung vom Server entfernen.
Ignorieren	Die infizierten Dateien einfach ignorieren. Sie sollten diese Aktion nicht als erste Aktion in der Liste auswählen, außer wenn sie ausdrücklich wünschen, dass ALLE verdächtigen Dateien hoch- und heruntergeladen werden. Dies stellt ein hohes Sicherheitsrisiko dar, denn einige dieser Dateien können Schädlinge beinhalten.

Klicken Sie **Änderungen Speichern**, um die Änderungen anzuwenden.

Individuelle Scan Profile erstellen

Stellen Sie fest, dass die mit den standard Scan-Profilen nicht zufrieden sind, können Sie individuelle Profile erstellen. Erstellen Sie ein neues Prüfprofil, indem Sie einen Namen in das Feld **Erstelle ein neues Profil** Feld und klicken Sie **Erstellen**. Das neu erstellte Profil wird erscheinen in der **Aktuelle Scan Profileö** Liste. Um zu lernen, wie man individuelle Profile konfiguriert, gehen Sie bitte zu *„Konfiguriere individuelle Scan-Profile“* (S. 79).

Konfiguriere individuelle Scan-Profile

Um die Einstellungen eines individuellen Scan Profils zu konfigurieren, müssen Sie es erst aus der LIste auswählen. Die folgenden Optionen können im Bereich **Profileinstellungen** konfiguriert werden:

Einstellungen	Beschreibung
Aktionen	Konfigurieren Sie die durchzuführenden Aktionen für durch BitDefender entdeckte Dateien die infiziert oder verdächtig sind.
Malware geprüft	Wählen Sie die Arten von Malware aus, nach denen BitDefender Suchen soll.
Erweiterte Scan Einstellungen	BitDefender Konfigurieren gepackte Dateien, Archive oder Dateien, die einen voreingestellten Wert überschreiten, zu prüfen.
Filter	Konfigurieren Sie BitDefender nur Dateien mit bestimmten Endungen zu prüfen.

Aktionen konfigurieren

Sie können verschiedene Aktionen für verdächtige und infizierte Dateien festlegen. Es gibt eine Aktionsliste die für jede Kategorie entdeckter Dateien angewendet werden kann (infiziert oder verdächtig). Wenn eine infizierte Datei entdeckt wird, so wird die erste Aktion auf der entsprechenden Liste angewendet. Wenn diese Aktion fehlschlägt, wird die nächste Aktion angewendet, usw.

Sie können die Reihenfolge, in der die Aktionen angewendet werden verändern. Wählen Sie eine Aktion und klicken Sie auf oder um sie in der Liste nach oben oder nach unten zu verschieben.

Aktionen für infizierte Dateien. Folgende Aktionen stehen für infizierte Dateien zur Verfügung:

Aktion	Beschreibung
Desinfizieren	Den Malware-Kode aus den infizierten Dateien entfernen. Das Desinfizieren kann in manchen Fällen fehlschlagen, beispielsweise wenn die infizierte Datei sich in speziellen Mail-Archiven befindet.
In Quarantäne verschieben	Infizierte Dateien von Ihrer ursprünglichen Position in den Quarantäne-Ordner verschieben. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko?
Löschen	Infizierte Dateien direkt und ohne Warnung vom Server entfernen.

Aktion	Beschreibung
Ignorieren	Die infizierten Dateien einfach ignorieren. ***Warnung*** Nicht als erste Aktion in der Liste **Ignorieren** einstellen. Dies zu tun erlaubt Benutzern alle infizierten Dateien hoch und runter zu laden.

Aktionen für verdächtige Dateien. Folgende Aktionen stehen für verdächtige Dateien zur Verfügung:

Aktion	Beschreibung
In Quarantäne verschieben	Verdächtige Dateien von der ursprünglichen Position in den Quarantäne-Ordner verschieben. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko?
Löschen	Verdächtige Dateien direkt und ohne Warnung vom Server entfernen.
Ignorieren	Die infizierten Dateien einfach ignorieren. Sie sollten diese Aktion nicht als erste Aktion in der Liste auswählen, außer wenn sie ausdrücklich wünschen, dass ALLE verdächtigen Dateien hoch- und heruntergeladen werden. Dies stellt ein hohes Sicherheitsrisiko dar, denn einige dieser Dateien können Schädlinge beinhalten.

Malwareprüfung konfigurieren

Um BitDefender einzustellen nicht nur nach Viren zu suchen, sondern auch nach Riskware, gehen Sie zu **Gescannte Malware** und wählen Sie **Nach Riskware scannen**. Wählen Sie die Arten von Riskware, nach denen BitDefender suchen soll, indem Sie die entsprechenden Kästchen markieren.

Optionen	Beschreibung
Anwendungen	Legitime Anwendungen prüfen, die als Spionage-Tool verwendet werden können, um schädliche Anwendungen oder andere Bedrohungen zu verbergen.
Adware	Scannt nach Adware Bedrohungen
Dialers	Scannt nach Anwendungen, die Premium Rufnummern anwählen.
Spyware	Scannt nach bekannten Spyware Bedrohungen

Fortgeschrittene Prüfeinstellungen konfigurieren.

Die folgenden fortgeschrittenen Einstellungen können im Bereich **Fortgescrittene Scan-Einstellungeb** konfiguriert werden:

- **Gepackte Dateien Scannen** - wählen Sie diese Option, um in gepackten Dateien zu scannen.
- **Scanne in Archiven** - wählen Sie diese Option, um in Archiven zu scannen. Geben sie die maximal zu scanende Archivtiefe an im Feld **Max Archivtiefeh**.
- **MAximal zu scanende Architiefe (KB)** - wählen Sie diese Option, um die maximale Archivtiefe anzugeben, die BitDefender Scannen wird. Geben Sie die Grösse in dem entsprechenden Feld ein.

Filter konfigurieren

Bestimmte Dateisorten sind anfälliger auf Viren als andere. So ist zum Beispiel das Risiko beim Ausführen einer `.exe` Datei höher, als beim Öffnen einer `.txt` oder einer `.gif` Datei.

Um festzulegen welche Dateisorten geprüft werden sollen, wählen Sie eine der folgenden Optionen im Bereich **Filter** :

Optionen	Beschreibung
Alle Endungen prüfen	Dateien werden unabhängig Ihres Typs geprüft.
Nur Anwendungsdateien prüfen	Nur Anwendungsdateien werden geprüft. Diese Kategorie ist auf Dateien mit den folgenden Erweiterungen beschränkt: `386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs;`

Optionen	Beschreibung
	`vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp` Viren werden normalerweise über Anwendungsdateien übertragen. Deshalb sollten diese Dateien immer überprüft werden.
Benutzerdefinierte Endungen prüfen	Nur Dateien mit den festgelegten Endungen werden geprüft. Sie müssen in das Editierfeld die Dateieendungen eingeben, die von BitDefender geprüft werden sollen, wobei diese mit Strichpunkten (";") zu trennen sind.
Alle bis auf die folgenden Endungen prüfen	Die Dateien mit den festgelegten Endungen werden NICHT geprüft. Sie müssen in das Editierfeld die Dateieendungen eingeben, die NICHT von BitDefender geprüft werden sollen, wobei diese mit Strichpunkten (";") zu trennen sind. Sie sollten Dateiearten, die bekannt für Vren sind nicht von der Prüfung ausschließen, wie beispielsweise `.exe`, `.doc`, `.ppt`, `.xls`, `.rtf`, `.pif`, `.bat` und Andere.

Nach Abschluss der Konfiguration des individuellen Profils, klicken Sie **Änderungen speichern**, um die Einstellungen zu speichern.

8.3. AntiViren-Schutz Prüfung

Um zu überprüfen ob BitDefender Antivirus funktionstüchtig ist können sie eine spezielle Test-Datei verwenden: *EICAR Standard Anti-virus Test*. EICAR steht für *European Institute of Computer Anti-virus Research*. Dies ist eine Test-Datei die von Antivirus-Produkten entdeckt wird.

Die Datei kann mit einem Texteditor erstellt werden, vorausgesetzt die Datei wird im Standard MS-DOS-ASCII-Format gespeichert und hat eine Länge von 68 Bytes. Sie könnte auch ein Größe von 70 Byte haben, wenn der Editor an das Dateiende ein CR/LF (Carriage Return/Linefeed) setzt.

Die Datei muss den folgenden Einzeiler enthalten :

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Speichern Sie die Datei unter irgendeinem Namen mit der Erweiterung .com (bspw. EICAR.COM) und laden Sie sie in ein Verzeichnis. BitDefender muss diese Datei als ein infiziertes Dokument behandeln.

Sie können die Webseite von EICAR unter http://eicar.com besuchen, die Beschreibung lesen und die Datei von einer der Locations der folgenden Webseite herunterladen: http://eicar.com/anti_virus_test_file.htm.

9. Aktualisierung

Jeden Tag werden neue Viren und Spyware entdeckt und identifiziert. Aus diesem Grund ist es von großer Bedeutung, dass Sie BitDefender stets mit den neuesten Virensignaturen versorgen.

Mit der Funktion des automatischen Updates kann BitDefender automatisch und regelmäßig aktualisiert werden, ohne dass der Administrator hierfür eingreifen müsste. Standardmäßig prüft BitDefender stündlich auf vorhandene Updates. Wenn neue Malware-Signaturen oder eine Engine entdeckt werden, wird Bitdefender diese automatisch herunterladen und installieren.

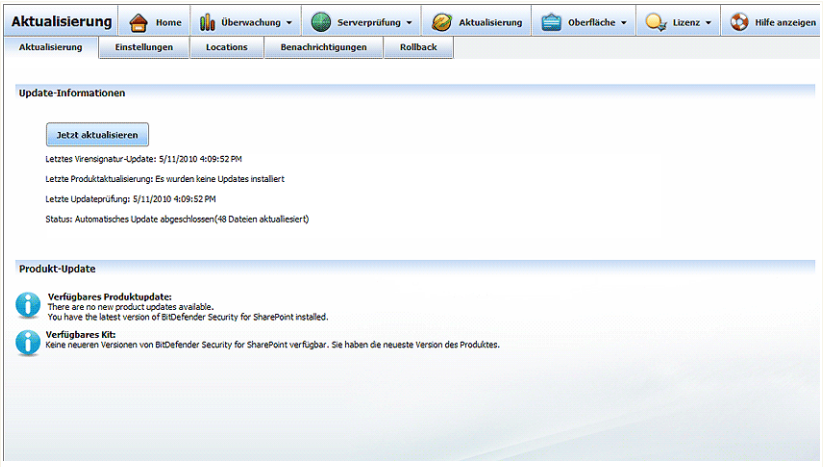
Das automatische Update kann jederzeit durchgeführt werden, indem Sie auf **Jetzt aktualisieren** im Bereich Update klicken oder indem Sie eine Geplante Update-Aufgabe erstellen.

Die Updates können folgendermaßen unterteilt werden:

- **Antivirus-Updates** - neue Virus- und Spyware-Signaturen sowie die Engines werden aktualisiert, um einen aktuellen Schutz zu gewährleisten.
- **Product updates** - wenn eine neue Version auf dem Markt erscheint, enthält diese zur Leistungssteigerung des Produkts neue Funktionen und Scantechniken.

9.1. Aktualisierung

Um Informationen zum Update Status zu erhalten und ob Updates verfügbar sind, klicken Sie im BitDefender Menu auf **Update**.



Aktualisierung

9.1.1. Update-Informationen

Im Abschnitt **Update Information**, Sie können den Update Status sehen und wann zuletzt nach einem Update gesucht und/oder durchgeführt wurde.

Wenn Sie den BitDefender sofort aktualisieren möchten, klicken Sie auf **Jetzt aktualisieren**. Das Update Modul wird die angegebenen Update Orte nach Updates durchsuchen. Wenn neue Malware-Signaturen oder eine Engine entdeckt werden, wird Bitdefender diese automatisch herunterladen und installieren.

9.1.2. Produkt-Update

Die Produktupdates unterscheiden sich von den Signatur Updates. Ihre Funktion ist die Lieferung neuer Bug-Fixes und Funktionen für das Produkt.

Es gibt zwei Arten von Updates für das Produkt:

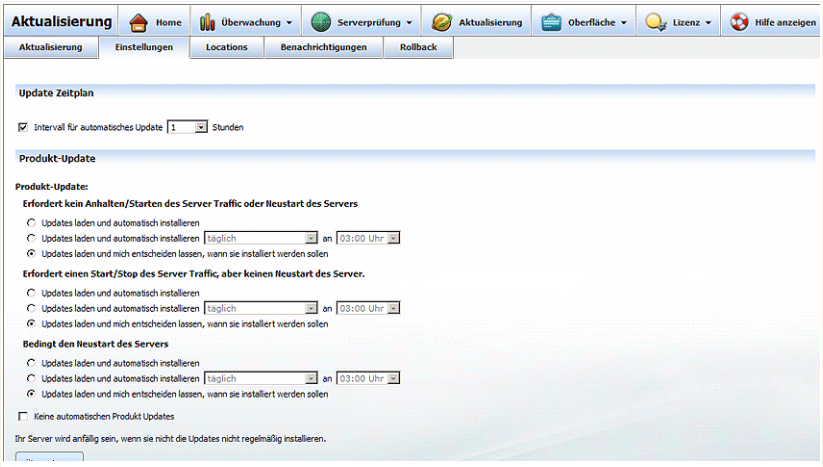
- **Produkt-Updates** - dies sind kumulative `EXE`-Dateien, die alle Dateien beinhalten, die seit der ersten Veröffentlichung des Produktes geändert wurden.
- **Version-Updates** - dies sind Installationspakete (Kits) mit einer neu veröffentlichten Version des Produktes.

Sobald Produkt-Updates verfügbar sind oder eine neuere Version erhältlich ist, wird hier die entsprechende Information angezeigt.

Standardmäßig werden Produkt-Updates und Version-Updates nicht automatisch installiert, da dies einen Neustart des Systems erfordern oder den Server-Datenverkehr unterbrechen könnte. Es wird empfohlen, die neuesten Updates so bald wie möglich zu installieren. Weitere Informationen zur Aktivierung und Konfiguration von automatischen Produkt-Updates finden Sie unter: „*Konfiguriere Produkt Updates*“ (S. 88).

9.2. Update-Einstellungen

Um die Update Häufigkeit und die Update Einstellungen zu konfigurieren, klicken Sie **Update** im BitDefender Menu und dann **Einstellungen**.


Aktualisierung
Home
Überwachung
Serverprüfung
Aktualisierung
Oberfläche
Lizenz
Hilfe anzeigen
Aktualisierung
Einstellungen
Locations
Benachrichtigungen
Rollback
Update Zeitplan
Intervall für automatisches Update 1 Stunden
Produkt-Update
Produkt-Update:
Erfordert kein Anhalten/Starten des Server Traffic oder Neustart des Servers
Updates laden und automatisch installieren
Updates laden und automatisch installieren täglich an 03:00 Uhr
Updates laden und mich entscheiden lassen, wann sie installiert werden sollen
Erfordert einen Start/Stop des Server Traffic, aber keinen Neustart des Server.
Updates laden und automatisch installieren
Updates laden und automatisch installieren täglich an 03:00 Uhr
Updates laden und mich entscheiden lassen, wann sie installiert werden sollen
Bedingt den Neustart des Servers
Updates laden und automatisch installieren
Updates laden und automatisch installieren täglich an 03:00 Uhr
Updates laden und mich entscheiden lassen, wann sie installiert werden sollen
Keine automatischen Produkt Updates
Ihr Server wird anfällig sein, wenn sie nicht die Updates nicht regelmäßig installieren.

Update-Einstellungen

9.2.1. Update-Planung konfigurieren

Es gibt zwei Mölichkeiten BitDefender Security for SharePoint regelmässig zu aktualisieren:

- **Verwendung des automatischen Updates.** Mit der Funktion des automatischen Updates kann BitDefender automatisch und regelmäßig aktualisiert werden, ohne dass der Administrator hierfür eingreifen müsste. Standardmäßig prüft BitDefender stündlich auf vorhandene Updates bei den festgelegten Update-Locations. Wenn neue Malware-Signaturen oder eine Engine entdeckt werden, wird Bitdefender diese automatisch herunterladen und installieren.

  Wichtig
  Lassen Sie das automatische Update aktiviert um gegen die aktuellsten Bedrohungen geschützt zu sein.

  Um die Frequenz zu überprüfen mit der BitDefender nach Updates such, wählen sie die Anzahl der Stunden zwischen 2 Suchen nach Updates au der Liste **Automatisches Update Interval**. Um die automatischen Updates zu deaktivieren, löschen Sie die Markierung im Kästchen **Automatic update interval**.

  Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.

- **Eine geplante Update-Aufgabe verwenden.** Mit geplanten Update-Aufgaben können die Malware-Signaturen und die Engines entsprechend eines eingestellten Zeitplans aktualisiert werden. Weitere Informationen finden Sie unter „*Update-Aufgaben*“ (S. 52).

Beachten Sie
Die geplanten Update-Aufgaben haben keinen Einfluss auf das automatische Update-Modul. Es führt weiterhin die regelmäßigen Überprüfungen der Update-Locations auf neue Signaturen durch.

9.2.2. Konfiguriere Produkt Updates

Produkt Updates regelmäßig zu installieren, ist für die Sicherheit Ihres Servers sehr wichtig. Abhängig von dem Grad der Beeinträchtigung des Servers, gibt es drei Arten von Produkt Updates:

- Produkt Updates, die kein anhalten des Server Verkehrs oder Neustart des Servers verlangen
- Produkt Updates, die ein Anhalten des Server Verkehrs verlangen, aber keinen Neustart des Servers
- Produkt Updates, die einen Neustart des Server verlangen

Um automatische Downloads und Installation für jede Art von Produkt Updates zu konfigurieren, wählen Sie eine der folgenden Optionen:

Updates laden und automatisch installieren
Wählen Sie diese Option und BitDefender wird automatisch Produkt Updates laden und installieren. Dies ist die empfohlene Wahl für Produkt Updates, die kein Anhalten des Server Verkehrs oder Neustart des Servers verlangen.

Updates automatisch laden und installieren... in...
Wählen Sie diese Option, wenn sie wollen, dass BitDefender verfügbare Updates zu einer gewissen Zeit installiert. Wählen Sie aus der Liste das Datum (Tag und Zeit) wann dies geschehen soll.

Auf diese Weise können Sie BitDefender konfigurieren Produkt Updates an Zeiten durchzuführen, zu denen die wenigsten Störungen der Server Aktivität zu erwarten sind (nachts bspw.)

Lade Updates und lasse mich entscheiden, wann diese installiert werden
Wählen Sie diese Option, wenn Sie wollen, dass BitDefender automatisch Produkt Updates lädt, sie aber entscheiden, wann sie installiert werden sollen. Dies ist die empfohlene Auswal für Produkt Updates, die ein Anhalten des Server Verkehrs und einen Neustart des Servers verlangen.

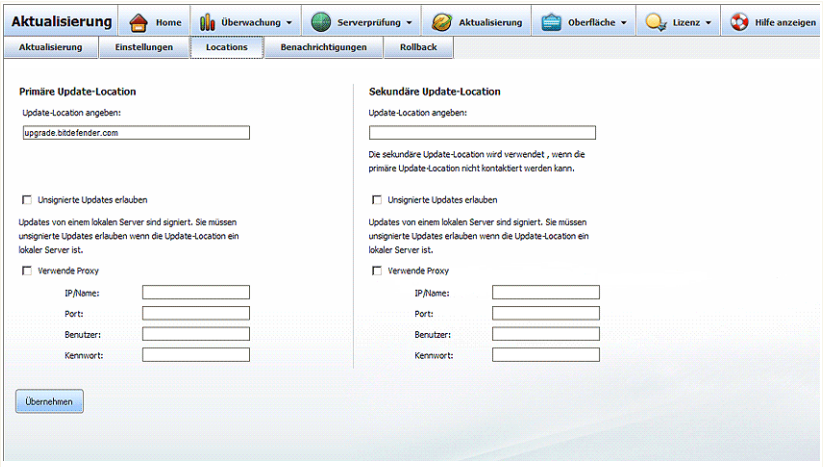
Um die automatischen Produkt Updates zu deaktivieren, wählen Sie **Keine automatischen Produkt Updates**.

Beachten Sie
Ihr Server wird gefährdet sein, wenn Sie nicht regelmässig Updates installieren.

Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.

9.3. Update Locations

Um die Update Orte festzulegen, klicken Sie **Update** im MitDefender Menu und dann **Orte**.



Update Locations

Die Updates können im lokalen Netzwerk, über das Internet, direkt oder über einen Proxy-Server durchgeführt werden.

Für zuverlässigere und schnellere Update können zwei Update-Locations angegeben werden: Eine **Erste Update-Location** und eine **Zweite Update-Location**. Die folgenden Optionen müssen für beide konfiguriert werden:

- **Update-Location** - geben Sie die Adresse des Update-Servers an. Standardmäßig lautet die erste Update-Location: `upgrade.bitdefender.com`.

  Wenn in Ihrem Netzwerk mehrere BitDefender-Produkte installiert sind, können Sie einen lokalen Server als primäre Update-Location und `upgrade.bitdefender.com` als sekundäre festlegen; die sekundäre wird verwendet, falls die primäre nicht erreichbar ist. So können Sie den Internet-Datenverkehr während der Aktualisierung reduzieren.

  Beachten Sie
  Die lokale Update-Location kann mit BitDefender Update Server (ein Teil von BitDefender Management Server) eingerichtet werden oder mithilfe eines Web-Servers wie Apache oder IIS veröffentlicht werden.

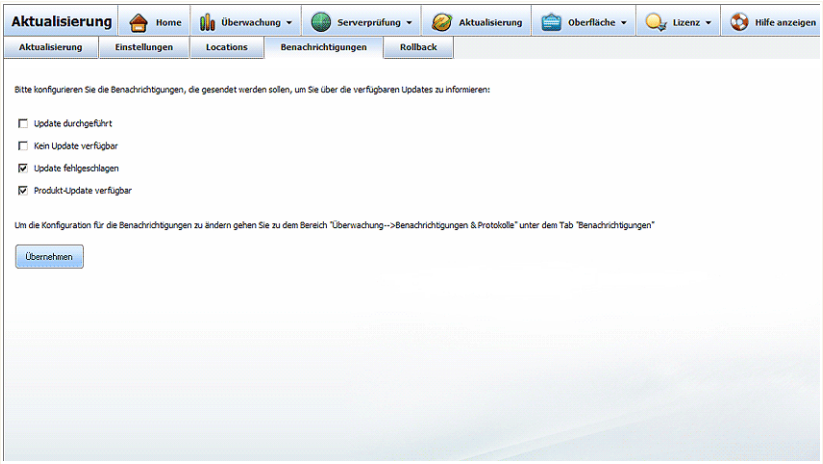
- **Unsignierte Updates erlauben** - wählen Sie diese Option, um Updates und Installationen von einem lokalen Server zu erlauben.

- **Proxy verwenden** - wählen Sie diese Option, falls Ihr Unternehmen einen Proxy-Server verwendet. Die folgenden Einstellungen müssen angegeben werden:
  - **IP/Name** - Geben Sie die IP-Adresse des Proxy-Servers ein.
  - **Port** - Geben Sie den Port ein, über den BitDefender die Verbindung zum Proxy-Server herstellt.
  - **Benutzername** - geben Sie einen für den Proxy-Server gültigen Benutzernamen ein.
  - **Passwort** - Geben Sie das Passwort für den zuvor angegebenen Benutzer ein.

Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.

9.4. Update Benachrichtigungen

BitDefender kann so eingestellt werden, dass Sie über bestimmte Ereignisse während des Betriebs benachrichtigt werden. Um festzulegen über welche Update-Ereignisse BitDefender Sie informieren soll, klicken Sie auf **Update**im BitDefender Menu und dann auf den Tab **Benachrichtigungen**.



Update Benachrichtigungen

Wählen Sie die Update-Ereignisse, über die Sie informiert werden möchten:

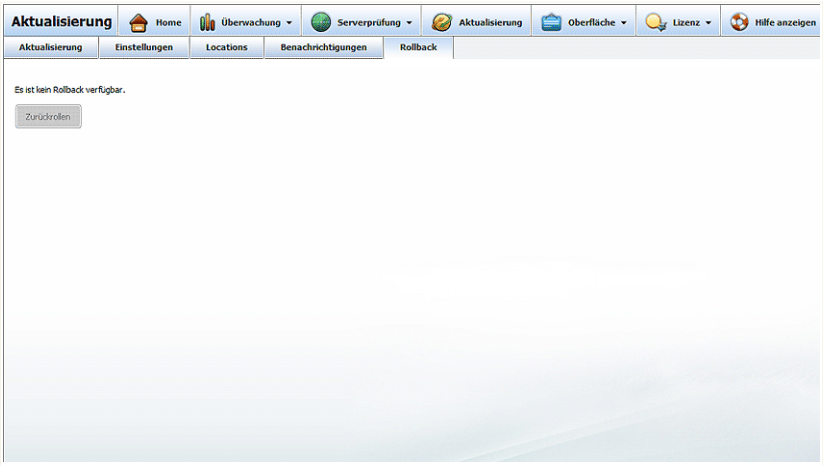
- **Update durchgeführt** - wenn ein Update durchgeführt wurde.
- **Kein Update verfügbar** - wenn kein Update zur Verfügung steht.
- **Update fehlgeschlagen** - wenn ein Fehler während eines Updates aufgetreten und dieses fehlgeschlagen ist.
- **Produkt-Update verfügbar** - Wenn ein Produkt-Update zur Verfügung steht.

Um BitDefender so einzustellen, dass das Auftreten eines Ereignisses protokolliert wird oder auch dass Sie darüber via Mail oder Net Send informiert werden, öffnen Sie **Benachrichtigungen&Protokolle** den Tab /emphasis>, Benachrichtigungen und konfigurieren Sie das entsprechende Ereignis. Weitere Informationen finden Sie hier: „*Ereignisse konfigurieren*“ (S. 37).

Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.

9.5. Update zurückrollen

Wenn Sie seit der Erstinstallation von BitDefender ein Produkt Update durchgeführt haben, können Sie mit Hilfe der **Rollback** Funktion, zu der vorigen Produkt Version zurückkehren. Diese Funktion ist sehr nützlich, falls Ihr Produkt sich unerwartet verhält. Um zu sehen, ob ein Rollback verfügbar ist, klicken Sie **Update** im BitDefender und dann **Rollback**.



Update zurückrollen

Wenn ein Rollback verfügbar ist, werden die aktuelle Produktversion und die Version, zu der Sie zurückrollen können, angezeigt. Klicken Sie **Roll Back** und bestätigen Sie Ihre Auswahl indem Sie im Bestätigungsfenster **Ja** klicken, um das Rollback auszuführen.

Wenn ein Rollback durchgeführt wurde, werden die aktuelle und die vorige Version angezeigt. Sie können den angegebenen Link benutzen, um zur neueren Version zurück zu Updaten.

10. Allgemein

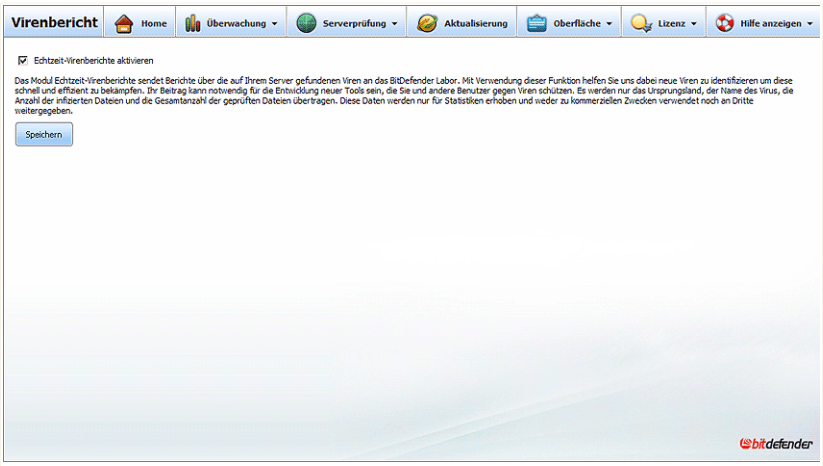
BitDefender kann hier so konfiguriert werden, dass Berichte an das BitDefender Labor bezüglich der Viren gesendet werden, die auf dem Server gefunden wurden, über Vorfälle während des Produktbetriebs und Sie Produkteinstellungen importieren/exportieren können.

10.1. Virenbericht

Mit den Virenberichten in Echtzeit können Berichte über die gefundenen Viren auf Ihrem Server an das BitDefender Labor gesendet werden, um uns dabei zu helfen, neue Viren zu identifizieren und Lösungen für diese zu finden. Ihr Beitrag könnte grundlegend für die Entwicklung neuer Tools sein, um Sie und Andere vor Virenbedrohungen zu schützen.

Diese Berichte enthalten keine persönlichen Daten wie Name, IP-Adresse oder andere Angaben. Die bereitgestellte Information enthält den Namen des Landes, den Virennamen, die Anzahl der infizierten Dateien sowie die Gesamtzahl aller geprüften Dateien. Die eigentlichen Berichte werden ausschließlich für eine statistische Auswertung verwendet. Sie werden weder Drittparteien vorgelegt, noch in irgendeiner Form kommerziell verwendet.

Um Echtzeit Virenberichte zu konfigurieren, gehen Sie zu **Virus Melden** unter **Allgemein** im BitDefender Menu.


Virenbericht
Home
Überwachung
Serverprüfung
Aktualisierung
Oberfläche
Lizenz
Hilfe anzeigen
Echtzeit-Virenberichte aktivieren
Das Modul Echtzeit-Virenberichte sendet Berichte über die auf Ihrem Server gefundenen Viren an das BitDefender Labor. Mit Verwendung dieser Funktion helfen Sie uns dabei neue Viren zu identifizieren um diese schnell und effizient zu bekämpfen. Ihr Beitrag kann notwendig für die Entwicklung neuer Tools sein, die Sie und andere Benutzer gegen Viren schützen. Es werden nur das Ursprungsland, der Name des Virus, die Anzahl der infizierten Dateien und die Gesamtanzahl der geprüften Dateien übertragen. Diese Daten werden nur für Statistiken erhoben und weder zu kommerziellen Zwecken verwendet noch an Dritte weitergegeben.
Speichern
bitdefender

Virenbericht

Virenberichte in Echtzeit sind standardmäßig deaktiviert. Um diese Funktion zu aktivieren, befolgen Sie folgende Schritte:

1. Wählen Sie **Virenberichte in Echtzeit aktivieren**.
2. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.

10.2. Vorfallsberichte

BitDefener Security für SharePoint enthält einen Vorfall Management Modul, welches es erlaubt während eines Produktabsturzes Berichte zu erstellen. Durch Ihre Zustimmung Vorfallsberichte an das BitDefender Labor zu senden, helfen Sie uns schnelle Problemlösungen zu finden. Sie könnten einen grpssen Beitrag zur der Entwicklung eines stabilen Produktes machen, dass Ihren Wünschen entspricht. Die Berichte werden nur für statistische Zwecke genutzt, die Daten werden niemals kommerziell genutzt oder an dritte weitergegeben.

Um Das Vorfallsverwaltungsmodul zu konfigurieren, gehen Sie im BitDefender Menu zu **Vorfälle Melden** unter **Allgemein**.

Berichtvorfälle
Home
Überwachung
Serverprüfung
Aktualisierung
Oberfläche
Lizenz
Hilfe anzeigen
Ich bin damit einverstanden Vorfallsberichte an das BitDefender Labor zu senden
Übernehmen
BitDefender Security for SharePoint enthält ein Vorfallsberichtsmanagement-Modul, dass bei Produktfehlfunktionen einen Bericht erstellt. Sie helfen uns schnelle Lösungen zu finden, wenn sie dem Verasand der Berichte an das BitDefender Labor zustimmen. Der Vorfallsbericht wird alleine zum Debugging verwendet. Die Daten werden weder für kommerzielle Zwecke verwendet, noch werden Sie an dritte weiter gegeben.

Vorfallsberichte

Standardmässig werden Berichte, die automatisch während eines Produktabsturzes erstellt wurden, nicht an das BitDefender Labor gesendet. Um BitDefender zu konfigurieren Vorfallsberichte an das BitDefender Labor zu senden, folgen Sie diesen Schritten:

1. Wählen Sie **Ich stimme zu, Berichte an das BitDefender Labor zu senden**.
2. Geben Sie Ihre E-Mail-Adresse an.
3. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.

10.3. importieren/exportieren der Management Konsole Einstellungen

Sie können die Einstellungen der Management Konsole importieren und exportieren. Dies hilft Ihnen andere BitDefender Security for SharePoint Produkte zu konfigurieren und konfigurierte Einstellungen wiederherzustellen, falls Sie Ihr Produkt reparieren oder neu installieren müssen.

10.3.1. Policy-Einstellungen exportieren

Um Produkteinstellungen zu exportieren, gehen Sie im BitDefender Menu zu **Einstellungen Exportieren** unter **Allgemein**.

Sie müssen nur **Exportieren** klicken und den Ordner wählen, in dem die Produkteinstellungsdatei gespeichert werden soll.

10.3.2. Policy-Einstellungen importieren

Um Produkteinstellungen zu importieren, gehen Sie im BitDefender Menu zu **Einstellungen Importieren** unter **Allgemein**.

Um zuvor gespeicherte Konsoleeinstellungen zu importieren, befolgen Sie diese Schritte:

1. Klicken Sie auf **Importieren**. Ein neues Fenster wird sich öffnen.
2. Finden und wählen Sie die Einstellungsdatei.
3. Klicke **Öffnen**, um Einstellungen zu importieren.

   Beachten Sie
   BitDefender schützt den SharePoint Server nicht, während Sie die Produkteinstellungen importieren. Deshalb wird es empfohlen, dass Sie den Dateiserver vom Netzwerk trennen, bevor Sie diesen Prozess ausführen.

4. Warten Sie, bis das Import Tool den Importieren-Prozess vollendet.
5. Sie werden vom Import Tool informiert sobald die Einstellungen erfolgreich importiert sind.

   Klicken Sie auf **Ausgang**, um dieses Fenster zu schließen.

11. Lizenz

BitDefender Security for Exchange verfügt über eine 30-tägige Testversion. Wenn Sie sich für BitDefender Security for SharePoint für Ihr Unternehmen entscheiden, kaufen und registrieren Sie die Vollversion. Sie sollten auch ein BitDefender Benutzerkonto erstellen, um sowohl den technischen Support als auch andere Serviceleistungen nutzen zu können.

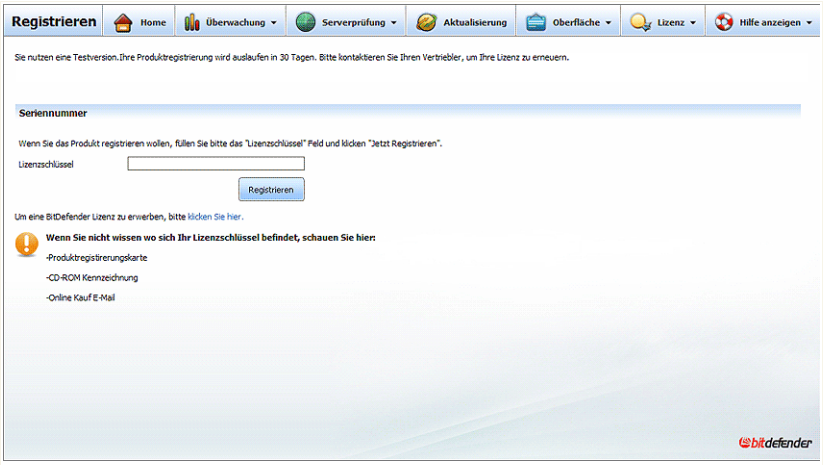
Beachten Sie
Wenn BitDefender Security for SharePoint von dem BitDefender Management Server verwaltet wird, wird die Registrierung des Produktes und des Benutzerkontos über die Management Konsole des BitDefender Management Server durchgeführt.

11.1. Kaufe die Vollversion des Produktes

Gehe zu **Kaufen** unter **Lizenz** im BitDefender Menu, wenn Sie die Vollversionfür BitDefender Security for SharePoint kaufen wollen. Dies wird eine Webseite öffnen, auf der Sie das Produkt kaufen können.

11.2. Produkt registrieren

Um BitDefender für SharePoint zu registrieren, gehen Sie im BitDefender Menu zu **Jetzt Registrieren** unter **Lizenz**.


Registrieren
Home
Überwachung
Serverprüfung
Aktualisierung
Oberfläche
Lizenz
Hilfe anzeigen
Sie nutzen eine Testversion.Ihre Produktregistrierung wird auslaufen in 30 Tagen. Bitte kontaktieren Sie Ihren Vertriebler, um Ihre Lizenz zu erneuern.
Seriennummer
Wenn Sie das Produkt registrieren wollen, füllen Sie bitte das "Lizenzschlüssel" Feld und klicken "Jetzt Registrieren".
Lizenzschlüssel
Registrieren
Um eine BitDefender Lizenz zu erwerben, bitte klicken Sie hier.
Wenn Sie nicht wissen wo sich Ihr Lizenzschlüssel befindet, schauen Sie hier:
-Produktregistrierungskarte
-CD-ROM Kennzeichnung
-Online Kauf E-Mail
bitdefender

Registrierung

Sie können den Status Ihrer Registrierung im oberen Teil der Seite sehen.

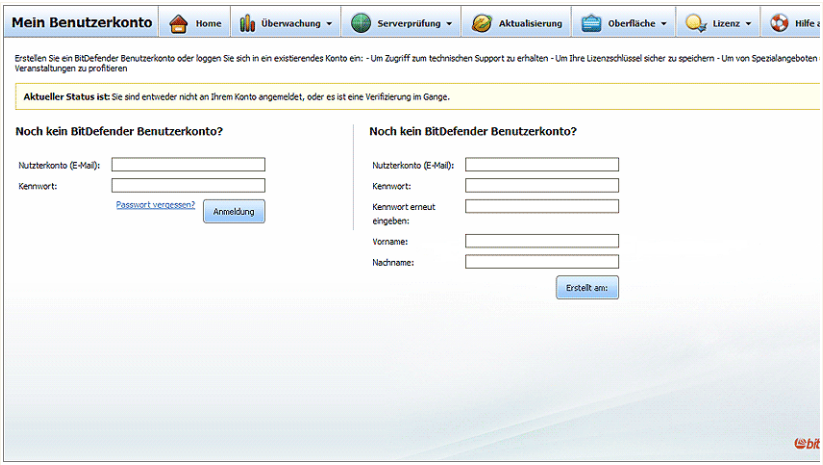
Wenn Sie keine Bitdefender-Lizenz besitzen, klicken Sie auf den angegebenen Link, um zu dem BitDefender Online-Shop zu gelangen und einen Lizenzschlüssel zu erwerben.

Um das Produkt zu registrieren, geben sie die Seriennummer in dem Feld **Lizenzschlüssel** ein und klicken Sie **Jetzt Registrieren**.

Beachten Sie
Falls der angegebene Lizenzschlüssel ungültig ist, werden Sie aufgefordert einen anderen Lizenzschlüssel einzugeben.

11.3. Ein BitDefender Benutzerkonto registrieren

Um ein BitDefender Benutzerkonto zu erstellen oder sich an einem anzumelden, gehen Sie im BitDefender Menu zu **Mein Konto** unter **Lizenz**.



Registrierung des Benutzerkontos

Sie können den aktuellen Stand Ihres Benutzerkontos in dem oberen Teil der Seite sehen. Gehen Sie nach Ihrer aktuellen Situation vor.

Ich habe noch kein BitDefender-Benutzerkonto

Um ein BitDefender Konto zu erstellen, müssen Sie nur die folgenden Informationen eingeben:

Beachten Sie
Die hier eingetragenen Daten bleiben vertraulich.

- **E-Mail** - geben Sie Ihre E-Mail Adresse an.

- **Passwort** - geben Sie ein Passwort für Ihr BitDefender-Benutzerkonto ein. Das Passwort sollte mindestens 4 Zeichen haben.
- **Passwort erneut eingeben** - geben Sie erneut das vorher angegebene Passwort ein.
- **Vorname** - geben Sie Ihren Vornamen ein.
- **Name** - geben Sie Ihren Namen ein.

Klicken Sie **Erstellen** um abzuschliessen.

Beachten Sie
Benutzen Sie die angegebene E-Mail Adresse und das Passwort um sich in Ihr Benutzerkonto unter folgendem Link einzuloggen: http://myaccount.bitdefender.com.

Um erfolgreich ein Benutzerkonto einzurichten müssen Sie zunächst Ihre E-Mail Adresse aktivieren. Überprüfen Sie hierzu Ihre E-Mails unter der angegebenen Adresse und folgen Sie den Instruktionen, die Sie vom BitDefender Registrierungsservice zugesandt bekommen haben.

Ich habe bereits ein BitDefender Benutzerkonto.

Wenn Sie bereits ein aktives Benutzerkonto haben, geben Sie die E-Mail Adresse und das Passwort Ihres Kontos in die entsprechenden Felder ein und klicken Sie **Anmelden**.

Beachten Sie
Wenn das angegebene Passwort nicht korrekt ist, so werden Sie dazu aufgefordert es erneut anzugeben, sobald Sie auf **Weiter** klicken.

Wenn Sie Ihr Passwort vergessen haben, klicken Sie **Passwort vergessen?** und folgen Sie den Instruktionen.

12. Hilfe

Hier können Sie auf die Produktdokumentation und auf die BitDefender Knowledge Base zugreifen sowie Versions Informationen.

Wenn Sie Informationen über den Gebrauch des Produktes benötigen, klicken Sie im BitDefender Menu auf **BD Security Hilfe** unter **Hilfe**. Dies wird die BitDefender Security for SharePoint Hilfe Datei öffnen.

Wenn Sie Probleme mit dem Produkt haben und Hilfe beim benötigen, klicken Sie **Support** und **Hilfe** im BitDefender Menu. Sie werden zum BitDefender Knowledge Base geleitet, wo Sie Dokumente zu den bekannten Problemen finden können und von wo aus Sie BitDefender Customer Care kontaktieren können. Für mehr Informationen über Hilfe, gehen Sie zu „Fehlerdiagnose und Problemlösung“ (S. 100).

Um VErsionsinformationen zu erhalten, klicken Sie **Über BD Security** unter **Hilfe** im BitDefender Menu. Hier können Sie die Versionsnummern der BitDefender Module zu sehen.

Fehlerdiagnose und Problemlösung

13. BitDefender Konfigurationsreparatur Tool

Wenn Sie Probleme mit BitDefender Security for SharePoint Servers haben, nutzen Sie bitte das BitDefender Konfigurationsreparatur-Tool um die letzte bekannte gute Konfiguration wiederherzustellen. Das BitDefender Konfigurationsreparatur Tool speichert die Konfigurationsdatei jede Stunde, so dass Sie es wenn erforderlich wieder herstellen können. Dieses Tool kann erfolgreich verwendet werden, um ein korruptes Konfigurationsdateiproblem zu befestigen, das in äußersten Situationen wie eine erzwungene durch eine Gedächtnislücke verursachte Systemstilllegung vorkommen kann.

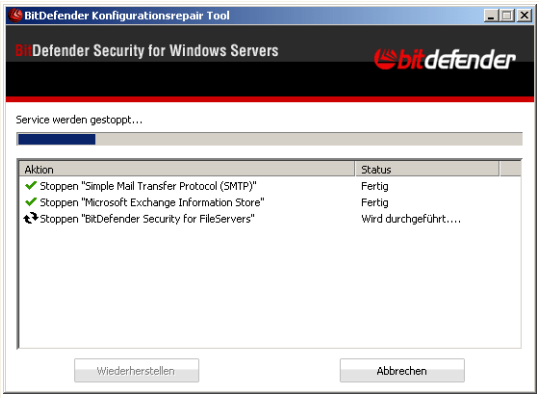
Um die letzte bekannte gute Version der Konfigurationsdatei wieder herzustellen, befolgen Sie diese Schritte:

1. Öffnen Sie das BitDefender-Konfigurationsreparatur-Tool auf folgende Weise: **Startmenü → Alle Programme → BitDefender Security for Windows Server → BitDefender-Konfigurationsreparatur-Tool**.

BitDefender Konfigurationsrepair Tool
BitDefender Security for Windows Servers
bitdefender
Das BitDefender Tool für die Konfigurationsreparatur hilft Ihnen bei der Wiederherstellung der letzten Ihnen bekannten gültigen Konfigurationen Ihrer BitDefender Security for Windows Server Produkte. Alle neuen Einstellungen, die nach der Speicherung der Konfiguration vorgenommen wurden, gehen verloren. Sie sollten dieses Tool nur verwenden, wenn Ihre derzeitige Konfiguration unvorteilhaft ist.
Klicken Sie auf "Wiederherstellen" und beginnen Sie mit der Wiederherstellung Ihrer Konfigurationsdateien, oder klicken Sie auf "Abbrechen" um diesen Dialog zu schließen und Ihre derzeitigen Einstellungen beizubehalten.
Wiederherstellen
Abbrechen

BitDefender Konfigurationsreparatur Tool

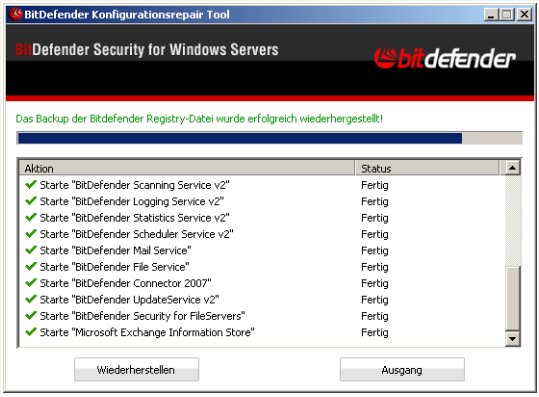
2. Klicken Sie auf **wiederherstellen**, um mit der Wiederhestellung der Sicherungskopie des Konfigurastionsfile zu beginnen
3. Bitte warten bis Bitdefender KonfigurationsReparatur Tool die Wiederherstzellungsprozess beendet.



Konfigurationsreparatur

Das fenster zeigt den Status des Wiederherstellungsprozesses Zuerst stoppt das BitDefender Konfigurationsreparatur Tool die Dienste von BitDefender Security for Servers Produkte, die auf dem System installiert sind (Dienste, die Anwendungen von Microsoft gehören, können auch angehalten werden; zum Beispiel, Microsoft Exchange Transport, wenn die BitDefender Security for Exchange installiert ist). Dann ersetzt das BitDefender Konfigurationsreparatur Tool die korrupte Konfigurationsdatei durch die Sicherungsdatei (eine ältere funktionierende Konfigurationsdatei).Schließlich startet das BitDefender Konfigurationsreparatur Tool wieder die vorher gestoppten Prozesse.

4. Das BitDefender Konfigurationsreparatur-Werkzeug informiert Sie, wenn die Sicherungkopie der Konfigurationsdatei erfolgreich wieder hergestellt worden ist.



Fertigstellen

Klicken Sie auf **Ausgang**, um dieses Fenster zu schließen.

14. Support

Als geschätzter Anbieter ist BitDefender stets bemüht, einen einmalig schnellen und sorgfältigen Support anzubieten. Sollten Probleme im Zusammenhang mit Ihrem BitDefender-Produkt auftreten oder Sie Fragen dazu haben, so wenden Sie sich bitte an unser Online-Support-Center. Dort gibt es verschiedene Ressourcen, mit deren Hilfe Sie schnell die richtige Lösung oder Antwort finden können. Sie können auch das Kundenbetreuungs-Team von BitDefender kontaktieren. Unsere Kundenbetreuer beantworten Ihre Fragen zügig und bieten Ihnen die benötigte Unterstützung.

Beachten Sie
Im Support-Center finden Sie weiterführende Informationen zu unseren Support-Leistungen und Support-Richtlinien.

14.1. BitDefender-Support-Center

Im BitDefender-Support-Center unter http://www.bitdefender.de/businesshelp unterstützen wir Sie in allen Belangen rund um Ihr BitDefender-Product.

Dabei stehen Ihnen verschiedene Ressourcen zur Verfügung, um die richtige Lösung oder Antwort zu finden:

- BitDefender Knowledge Base
- BitDefender Support-Forum
- Video Tutorials
- Produktdokumentation

Weitere Informationen über Computersicherheit, BitDefender-Produkte und unsere Firma finden Sie über Ihre Lieblingssuchmaschine.

14.1.1. BitDefender Knowledge Base

Bei der BitDefender Knowledge Base handelt es sich um eine Wissensdatenbank mit Informationen rund um Bitdefender Produkte. In leicht verständlicher Form bietet die Knowledge Base Informationen, Anleitungen und Berichte über neue Patches und behobene Probleme.Ebenfalls enthalten sind empfohlene Vorgehensweisen bei der Verwendung von Bitdefender Produkten und allgemeine Informationen wie z.B. Präventionsmaßnahmen vor Viren und anderen Schädlingen.

Die BitDefender Knowledge Base ist zudem öffentlich zugänglich und komplett durchsuchbar. Durch diese Art der Informationsbereitstellung bieten wir unseren Kunden eine weitere Möglichkeit, technische Grundlagen und Fachwissen über unsere Produkte zu erlangen.

Die BitDefender-Knowledge-Base für Unternehmensprodukte ist jederzeit unter http://www.bitdefender.de/businesshelp erreichbar.

14.1.2. BitDefender Support-Forum

Das BitDefender Support Forum bietet Anwendern eine Möglichkeit, Hilfe zu erhalten oder anderen Hilfestellung zu geben. Hier können Sie Ihre Probleme und Fragen rund um Ihr BitDefender-Produkt posten.

Support-Techniker von BitDefender überwachen neue Forumeinträge, um Ihnen helfen zu können. Außerdem können Sie eine Antwort auf Ihre Frage oder einen Lösungsvorschlag von einem bereits erfahrenen BitDefender-Anwender erhalten.

Bevor Sie einen Eintrag ins Forum stellen, suchen Sie bitte im Forum nach einem ähnlichen oder verwandten Themenbereich.

Das BitDefender Support Forum finden Sie unter http://forum.bitdefender.com. Es steht in fünf Sprachen zur Verfügung: Englisch, Deutsch, Französisch, Spanisch und Rumänisch. Mit einem Klick auf **Business Protection** gelangen Sie in den Bereich Unternehmensprodukte.

14.1.3. Video Tutorials

Die Video Tutorials leiten Sie Schritt für Schritt durch die Konfiguration des Produkts.

Ziel ist es, die Abhängigkeit von professioneller Unterstützung zu beenden und im Gegenzug die notwendigen Informationen zur Verwendung und Konfigurationen von BitDefender-Produkten in Video-Tutorials zur Verfügung zu stellen. So müssen Sie nicht erst beim BitDefender-Support anrufen, um Hilfe zu erhalten oder versuchen, komplizierte Verfahren umzusetzen. Sehen Sie sich ein Video-Turorial an und folgen Sie den beschriebenen Schritten.

Die Video-Tutorials für die Unternehmensprodukte finden Sie unter Support-Center > Video-Tutorials.

14.1.4. Produktdokumentation

Die Produktdokumentation ist die umfassendste Informationsquelle rund um Ihr Produkt.

Unter Support-Center > Dokumentation stehen die neuesten Versionen der Dokumentationen für die BitDefender-Unternehmensprodukte zum Download bereit.

14.2. Hilfe anfordern

Nutzen Sie das Online-Support-Center, um Unterstützung anzufordern:

1. Rufen Sie http://www.bitdefender.de/businesshelp auf.
2. Durchsuchen Sie die Knowledge-Base nach Artikeln, die eine Lösung für Ihr Problem enthalten könnten.
3. Lesen Sie die relevanten Artikel oder Dokumente und probieren Sie die vorgeschlagenen Lösungen aus.

4. Sollten Sie keine entsprechende Lösung finden können, klicken Sie auf **Contact Us** im Menü auf der linken Seite.
5. Im Kontaktformular können Sie ein E-Mail-Support-Ticket eröffnen oder auf weitere Kontaktoptionen zugreifen.

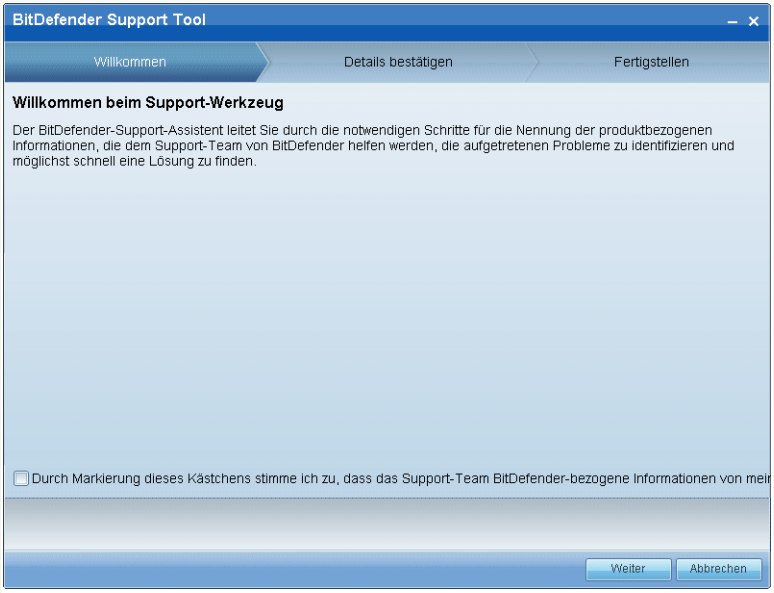
Nähere Kontakt-Informationen finden Sie unter „*Kontaktinformation*“ (S. 108).

14.3. BitDefender Support Tool

The BitDefender Support Tool creates a zip archive of files required by our support technicians to troubleshoot BitDefender Security for SharePoint.

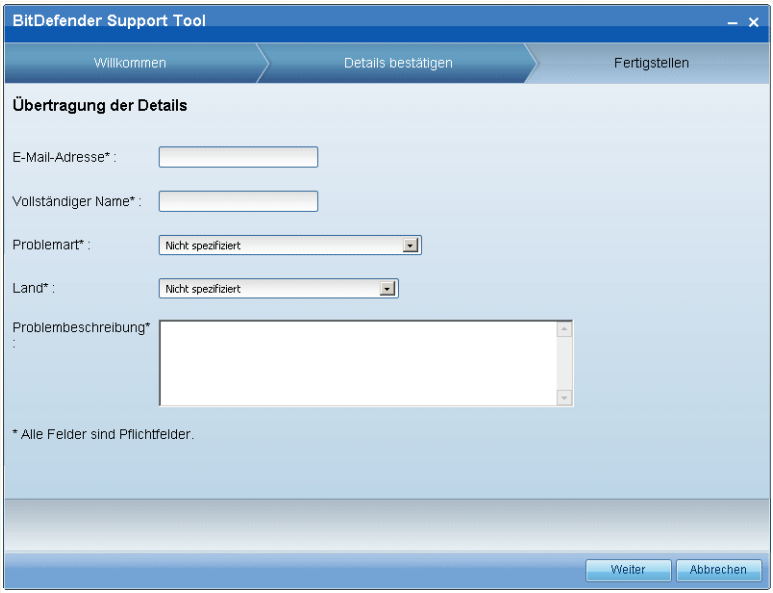
Um das Support Tool zu benutzen, folgen Sie diesen Schritten:

1. Öffnen Sie das BitDefender-Support-Tool über den folgenden Pfad: **Startmenü → Alle Programme → BitDefender Security for Windows Servers → BitDefender-Support-Tool**.


BitDefender Support Tool
Willkommen
Details bestätigen
Fertigstellen
Willkommen beim Support-Werkzeug
Der BitDefender-Support-Assistent leitet Sie durch die notwendigen Schritte für die Nennung der produktbezogenen Informationen, die dem Support-Team von BitDefender helfen werden, die aufgetretenen Probleme zu identifizieren und möglichst schnell eine Lösung zu finden.
Durch Markierung dieses Kästchens stimme ich zu, dass das Support-Team BitDefender-bezogene Informationen von mei
Weiter
Abbrechen

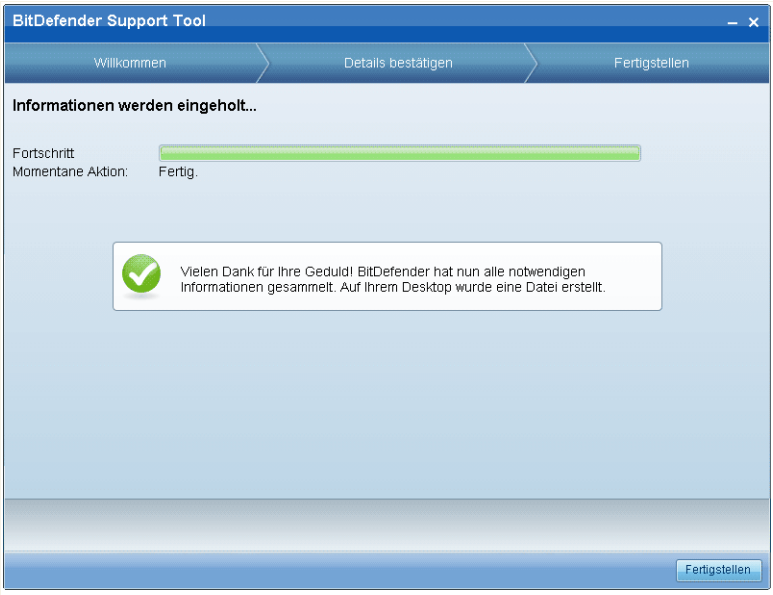
BitDefender Support Tool

2. Markieren Sie das Zustimmungskästchen und klicken Sie auf **Weiter**.



Übertragung der Details

3. Geben Sie in das Formular die nötigen Daten ein:
   a. Geben Sie Ihre E-Mail-Adresse ein.
   b. Geben Sie Ihren Namen ein.
   c. Wellen Sie aus dem Menü die Art des Problems, das aufgetreten ist.
   d. Wählen Sie Ihr Land aus dem entsprechenden Menü.
   e. Beschreiben Sie im Textfeld das Problem, dass aufgetreten ist.
4. Klicken Sie auf **Weiter**. Das Support Tool sammelt Produktinformationen, Informationen zu anderen Anwendungen, die auf ihrem System installiert sind sowie die Software und Hardware Konfiguration.
5. Warten Sie, bis der Vorgang beendet ist.



Fertigstellen

Es wurde ein ZIP-Archiv auf Ihrem Desktop erstellt. Klicken Sie auf **Beenden**, um das Fenster zu schließen.

Sie können das .zip Archiv zusammen mit Ihrer Supportanfrage senden, um die Zeit zur Lösung Ihrer Anfrage zu reduzieren.

15. Kontaktinformation

Effiziente und kundenorientierte Kommunikation ist der Schlüssel zu einem erfolgreichen Geschäftsmodell.Seit mehr als 10 Jahren überbietet BITDEFENDER konstant die bereits hochgesteckten Erwartungen unserer Kunden und Partner und diese Tradition wollen wir auch in Zukunft fortführen. Für jedwede Fragen stehen wir Ihnen gerne zur Verfügung.

15.1. Kontaktadressen

Vertrieb: vertrieb@bitdefender.de
Support-Center: http://www.bitdefender.de/businesshelp
Dokumentation: documentation@bitdefender.com
Lokale Vertriebspartner: http://www.bitdefender.de/partners
Partner Proogramm: vertrieb@bitdefender.de
Media Relationspresse@bitdefender.de
Jobs: jobs@bitdefender.de
Virus Einsendungen: virus_submission@bitdefender.com
Spam Einsendungen: spam_submission@bitdefender.com
Report Abuse: abuse@bitdefender.com
Webseite: http://www.bitdefender.de

15.2. Händler vor Ort

Die BitDefender Händler stehen für Fragen und Informationen in ihren jeweiligen Regionen jederzeit zur Verfügung, sowohl für vertriebliche als auch für allgemeine Anfragen.

So finden Sie einen BitDefender Distributor in Ihrem Land:

1. Rufen Sie http://www.bitdefender.de/site/Partnership/list auf.
2. Die Kontaktinformationen der lokalen BitDefender-Vertriebspartner sollten automatisch angezeigt werden. Sollte dies nicht der Fall sein, so wählen Sie Ihr Land aus, um die Informationen anzuzeigen.
3. Falls Sie in Ihrem Land keinen BitDefender Distributor finden, können Sie uns gerne unter vertrieb@bitdefender.de kontaktieren. Bitte schreiben Sie uns Ihre Email in englischer Sprache, damit wir Ihnen umgehend helfen können.

15.3. BitDefender Geschäftsstellen

Die BitDefender Niederlassungen stehen für Fragen und Informationen in ihren jeweiligen Regionen jederzeit zur Verfügung, sowohl für vertriebliche als auch für allgemeine Anfragen. Die genauen Kontaktdaten und Adressen finden Sie in der unten stehenden Auflistung.

15.3.1. Deutschland

BitDefender GmbH
Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
Telefon (Geschäftsstelle&Vertrieb): +49 (0)2301 91 84 222
Telefon (Technischer Support): +49 (0)2301 91 84 444
Vertrieb: vertrieb@bitdefender.de
Webseite: http://www.bitdefender.de
Support-Center: http://www.bitdefender.de/businesshelp

15.3.2. Rumänien

BITDEFENDER SRL
West Gate Park, Building H2, 24 Preciziei Street
Bucharest, Sector 6
Fax: +40 21 2641799
Telefon (Vertrieb&Technischer Support): +40 21 2063470
Vertrieb: sales@bitdefender.ro
Webseite: http://www.bitdefender.ro
Support-Center: http://www.bitdefender.ro/businesshelp

15.3.3. USA

BitDefender, LLC
PO Box 667588
Pompano Beach, Fl 33066
United States
Telefon (Vertrieb&Technischer Support): 1-954-776-6262
Vertrieb: sales@bitdefender.com
Web: http://www.bitdefender.com
Support-Center: http://www.bitdefender.com/businesshelp

15.3.4. Großbritannien und Irland

Business Centre 10 Queen Street
Newcastle, Staffordshire
ST5 1ED
UK
Telefon (Vertrieb&Technischer Support): +44 (0) 8451-305096
E-Mail: info@bitdefender.co.uk
Vertrieb: sales@bitdefender.co.uk
Webseite: http://www.bitdefender.co.uk
Support-Center: http://www.bitdefender.co.uk/businesshelp

15.3.5. Spain

BitDefender España, S.L.U.
Avda. Diagonal, 357, 1º 1ª
08037 Barcelona
España
Fax: (+34) 93 217 91 28
Telefon (Geschäftsstelle&Vertrieb): (+34) 93 218 96 15
Telefon (Technischer Support): (+34) 93 502 69 10
Vertrieb: comercial@bitdefender.es
Webseite: http://www.bitdefender.es
Support-Center: http://www.bitdefender.es/businesshelp

Glossar

Adware

Adware ist häufig mit einer Absenderanwendung kombiniert, die kostenlos ist, solange der Nutzer die Adware akzeptiert. Adware Anwendungen müssen in der Regel installiert werden, nachdem der Nutzer einer Lizenzvereinbarung zugestimmt hat. In der Lizenzvereinbarung wird auch der Zweck der Anwendung genannt und somit liegt keine Rechtswidrigkeit vor.

Allerdings können Popup-Anzeigen mit der Zeit sehr lästig werden und in manchen Fällen die Systemperformance beeinträchtigen. Zudem kann aufgrund der Daten, die manche dieser Programme sammeln, die Privatsphäre von Nutzern verletzt werden, die sich über die Bedingungen in der Lizenzvereinbarung nicht völlig im Klaren waren.

AktiveX

AktiveX ist ein Programmuster, dass von anderen Programmen und Betriebssystemkomponenten unter Windows aufgerufen werden kann.Die AktiveX Technologie wird von Microsofts Internet Explorer benutzt, damit interaktive Webseiten eher wie Programme und nicht wie statische Seiten angezeigt werden.Mit AktiveX können die Benutzer z.B. Fragen stellen oder beantworten, Buttons verwenden, oder verschiedenartige Interaktionen mit der Webseite herstellen.AktiveX Controls werden oft in Visual Basic geschrieben.

Erwähnenswert ist, dass bei AktiveX die Sicherheitskontrollen fehlen, deshalb raten Computersicherheitsexperten davon ab, AktiveX über das Internet zu nutzen.

Aktualisierung

Neue Softwareversionen oder Hardwareprodukte, die eine ältere Version ersetzen.Die Update-Installationsroutine sucht nach älteren Versionen auf dem Rechner, da sonst kein Update installiert werden kann.

BitDefender hat sein eigenes Update Modul, welches das manuelle oder automatische Prüfen nach Updates ermöglicht.

Arbeitsspeicher

Interne Speicherzonen im Rechner.Der Begriff Arbeitsspeicher bedeutet Datenträger in Form von sehr schnellen Chips.Das Wort Speicher ist der Speicherplatz, der sich auf Magnetbändern oder Datenträgern befindet.Jeder Rechner hat eine gewisse Menge Arbeitsspeicher.Dieser wird auch Hauptspeicher oder RAM genannt.

Archive

Ein Datenträger, ein Magnetband oder ein Ordner mit Dateien, die von einer Datensicherung/BackUp erzeugt wurden.

Eine Datei, die eine oder mehrere Dateien in einem komprimierten Format enthält.

Backdoor (Hintertür)

Eine Sicherheitslücke eines Systems, die der Entwickler oder Verwalter absichtlich hinterlässt.Der Grund dafür muss nicht immer bösartig sein.Manche Betriebssysteme haben schon bei der Fabrikation privilegierte Konten, damit diese von den Kundendienst-Technikern oder Programmierern der Hersteller benutzt werden können.

Befehlszeile

Die Befehlszeile ist eine zeichenorientierte Benutzerschnittstelle. Die Kommunikation zwischen Benutzer und Computer findet ausschließlich durch die Eingabe von bestimmten Befehlen statt, die sich aus einzelnen Buchstabenfolgen zusammensetzen. Als Eingabegerät wird eine Tastatur benutzt. Die Verwendung einer Maus ist nicht möglich. Auf der Befehlszeile werden die einzelnen Anweisungen in einer bestimmten Befehlssprache eingegeben, die vom Computer und seiner Software ausgewertet und mit den entsprechenden Ergebnissen auf dem Ausgabegerät (meistens ein Monitor) wieder an den Benutzer übergeben werden.

Bootsektor

Der erste Sektor einer Festplatte oder Diskette.Hier liegen Daten, die das Betriebssystem zum Booten (Starten) braucht.

Bootvirus

Ein Virus, der den Bootsektor einer Festplatte oder eines Diskettenlaufwerks infiziert.Beim Versuch von einer Diskette, die mit einem Bootvirus infiziert ist, zu booten wird dieser im Arbeitsspeicher aktiviert.Bei jedem Neustart wird der Virus so im Arbeitsspeicher aktiviert und überträgt sich auf eingelegte Wechselmedien.

Cookie

In der Internetindustrie werden Cookies als kleine Dateien beschrieben, die Daten über einzelne Computer enthalten und die von den Werbern analysiert und verwendet werden, um die Interessen und Vorlieben der Benutzer herauszufinden.Die Cookie-Technologie wurde deshalb weiter entwickelt, damit der Benutzer nur solche Werbung zugeschickt bekommt, die seinen Interessen dient.Für viele ist es aber wie ein zweischneidiges Messer.Einerseits ist es wirksam und sachbezogen, da man nur Anzeigen, an denen man interessiert ist, betrachten kann, anderseits heißt es dem Benutzer "auf die Spur zu kommen" und ihn auf Schritt und "Klick " zu verfolgen.Es ist verständlich, dass der Datenschutz ein umstrittenes Thema ist und viele sich von dem Begriff als SKU-Nummern (die Streifencodes auf den Packungen, die im Geschäft an der Theke gescannt werden) betrachtet zu werden, angegriffen fühlen.Auch wenn dieser Gesichtspunkt extrem erscheint ist er manchmal korrekt.

Dateierweiterung

Der Teil hinter dem Punkt im Dateinamen. Die Erweiterung oder Extension beschreibt die Art der Daten, die in einer Datei gespeichert sind.

Viele Betriebssysteme benutzen Dateierweiterungen, z.B. Unix, VMS, MS-DOS.Sie enthalten gewöhnlich ein bis zwei Buchstaben (alte Betriebssysteme können nicht mehr als drei Buchstaben unterstützen), Beispiele dafür sind "c" für C-Quellcode, "ps" für PostScript oder "txt" für beliebige Texte.Windows zeigt bei ihm bekannten Dateitypen keine Dateierweiterung in der graphischen Benutzeroberfläche an, stattdessen wird häufig ein Symbol verwendet.

Download

Kopiert Daten (gewöhnlich eine ganze Datei) von einer Hauptquelle auf ein Peripheriegerät.Der Begriff bezeichnet oft den Kopiervorgang von einem Online Service auf den eigenen Rechner.Download oder Herunterladen kann auch das Kopieren einer Datei von einem Netzwerkserver auf einen Netzwerkrechner bedeuten.

Durchsuchen

Kurzform für Web-Browser, eine Softwareanwendung, die zum Lokalisieren und Anzeigen von Webseiten verwendet wird.Die bekanntesten Browser sind Netscape Navigator und Microsoft Internet Explorer.Beide sind graphische Browser, das heißt sie können sowohl Grafiken als auch Texte anzeigen.Weiterhin können die meisten Browser Multimedia-Informationen wie Klang- und Videodateien anzeigen, wobei sie für diverse Formate Plug-Ins (zusätzliche Softwarekomponenten) benutzen.

E-Mail

Elektronische Post. Ein Dienst, der Nachrichten an andere Rechner über ein lokales oder ein globales Netzwerk übermittelt.

E-Mail Client

Ein E-Mail Client ist eine Anwendung, die das Senden und Empfangen von E-Mails ermöglicht.

Ereignisanzeige

Ereignisse oder Erscheinungen, die in einem Programm vorkommen.Ereignisse können Benutzeraktionen, wie zum Beispiel Mausklicks oder Tastatureingaben, oder Systemereignisse, wie zum Beispiel ungenügender Speicher, sein.

Fehlalarm

Erscheint, wenn ein Virenscanner eine Datei als infiziert erkennt, obwohl dies nicht der Fall ist. Kann bei heuristischem Virenprüfen auftreten.

Heuristik

Eine Methode, um neue Viren zu identifizieren.Diese Prüfmethode beruht nicht auf spezifische Virussignaturen.Der Vorteil einer heuristischen Prüfung ist, dass man nicht von einer neuen Virusvariante getäuscht werden kann.Manchmal kann auch ein verdächtiger Code in einemnormalen Programm gemeldet werden, ein sogenannter Fehlalarm wird angezeigt.

IP

Internet Protocol - Das TCP/IP Protokoll ist verantwortlich für die korrekte IP Adressierung und die korrekte Zustellung der Datenpakete.

Java Applet

Ein Java Programm, das nur auf Webseiten läuft.Um ein Applet auf einer Webseite zu benutzen, gibt man den Namen und die Größe (Länge und Breite in Pixel) des Applets an.Wenn die Webseite abgerufen wird, lädt der Browser das Applet vom Server herunter und führt es auf der Benutzermaschine (dem Client) aus.Applets sind keine Anwendungen, da sie von strengen Sicherheitsprotokollen gesteuert werden.

Obwohl Applets auf dem Client laufen, können diese keine Daten auf der Clientmaschine lesen oder schreiben.Zusätzlich sind die Applets weiter begrenzt, so dass sie nur Daten aus der Domäne lesen und beschreiben können, die sie unterstützen.

Komprimierte Programme

Eine Datei in einem komprimierten Format.Viele Betriebssysteme und Anwendungen enthalten Befehle, die das Komprimieren einer Datei ermöglichen, so dass diese weniger Speicherplatz benötigt.Zum Beispiel: Angenommen Sie haben einen Text, der 10 aufeinander folgende Leerzeichen enthält.Normalerweise nehmen diese 10 Bytes Speicherplatz ein.

Ein Programm, das Dateien komprimiert, würde die Leerzeichen durch ein spezielles Zeichen „Leerzeichenreihe“ ersetzen, gefolgt von der Zahl der Leerzeichen, die ersetzt wurden.In diesem Fall sind nur noch zwei Bytes notwendig statt zehn.Das wäre ein Beispiel für eine Komprimierungstechnik, es gibt aber noch viele andere.

Laufwerk

Ein Gerät, das rotierende Speichermedien lesen und beschreiben kann.

Ein Festplatten-Laufwerk liest und beschreibt Festplatten.

Ein Disketten-Laufwerk liest und beschreibt Disketten.

Laufwerke können sowohl interner (im Rechner eingebaut) als auch externer (in einem Gehäuse, das an den Rechner angeschlossen wird) Art sein.

Logdatei (Berichtsdatei)

Eine Datei, die stattgefundene Aktivitäten aufzeichnet.Zum Beispiel speichert BitDefender eine Logdatei mit die geprüften Pfaden, Ordnern und der Archivanzahl, aber auch die geprüften, infizierten oder verdächtigen Dateien.

Makrovirus

Eine Virusform, die in einem Dokument als eingebettetes Makro verschlüsselt wird.Viele Anwendungen, wie Microsoft Word und Excel, unterstützen mächtige Makrosprachen.

Diese Anwendungen ermöglichen das Einbetten eines Makros in ein Dokument, welches dann bei jedem Öffnen des Dokuments ausgeführt wird.Ein Makro ist eine Aufzeichnung des Ablaufs von Routineaufgaben innerhalb des makrofähigen Programms, das dann immer wieder verwendet werden kann.

Nicht heuristisch

Diese Prüfmethode beruht auf einer spezifischen Virussignatur.Der Vorteil einer nicht heuristischen Prüfung ist, dass diese nicht von einem Scheinvirus getäuscht werden kann, und dass dieser keinen falschen Alarm auslöst.

Pfad

Zeigt die Stelle an, an der sich eine Datei in einem Rechner befindet.Diese Pfadangaben enthalten gewöhnlich den hierarchischen Aufbau des Dateiverzeichnisses: Laufwerke, Ordner, Unterverzeichnisse, die Datei und ihre Erweiterung.

Der Weg zwischen zwei Punkten, wie zum Beispiel der Kommunikationskanal zwischen zwei Rechnern.

Phishing

Dabei wird eine E-Mail mit einer betrügerischen Absicht an einen Nutzer gesendet.Der Inhalt dieser E-Mail gibt vor, von einem bekannten und seriös arbeitenden Unternehmen zu stammen.Zweck dieser E-Mail ist es dann, private und geheime Nutzerdaten zu erhalten, worauf der Absender beabsichtigt, die Identität des Nutzers anzunehmen.Die E-Mail führt den Benutzer dann auf eine Webseite, in der er aufgefordert wird, vertrauliche Daten wie Kreditkartennummern, TAN's oder PIN's preiszugeben.Dies soll aus Gründen der Aktualisierung geschehen.Diese Webseiten sind jedoch gefälscht und wurden eigens für den Diebstahl dieser Daten eingerichtet.

Polymorpher Virus

Ein Virus, der seine Form mit jeder Datei, die er infiziert, ändert.Da diese Viren kein beständiges binäres Muster haben, sind sie sehr schwer zu erkennen.

Rootkit

Bei einem Rootkit handelt es sich um einen Satz von Softwarewerkzeugen die einem Administrator Low-End Zugriff zu einem System verschaffen. Rootkits traten zunächst nur auf UNIX-Systemen auf und haben im Laufe der Zeit auch Ihren Einzug auf Linux- und Windows-Systemen gehalten.

Die Hauptaufgabe eines Rootkits besteht darin, seine Existenz zu verstecken indem Prozesse und Dateien versteckt werden, Anmeldedaten und Berichtsdateien zu fälschen und jegliche Art von Daten abzufangen.

Rootkits zählen von Haus aus nicht zu schadensverursachender Software da Sie keine Schadroutinen besitzen. Jedoch verändern Sie die vom Betriebssystem zurückgegebenen Daten und verstecken auf diese Weise ihre Präsenz. Dennoch kann über ein solches Rootkit schädliche Software nachträglich eingeschleust werden und auch der wirtschaftliche Schaden ist nicht zu unterschätzen.

Schnittstelle

Stelle eines Rechners, an die ein Gerät angeschlossen werden kann.Rechner haben verschiedenartige Schnittstellen.Intern gibt es Schnittstellen zum Anschluss von Festplatten, Grafikkarten und Tastaturen.Extern haben Rechner Schnittstellen zum Anschluss von Modems, Druckern und anderen Peripheriegeräten.

In TCP/IP und UDP Netzwerken, ein Endpunkt zu logischen Verbindungen.Die Schnittstellennummer gibt die Art der Schnittstelle an.Zum Beispiel, Schnittstelle 80 wird für HTTP Traffic verwendet.

Script

Ein anderer Begriff für Makro- oder Batchdatei. Ein Skript ist eine Befehlsliste, die ohne Benutzereingriff ausgeführt werden kann.

Spam

Junk-E-Mail oder Junk-Postings in Newsgroups.Im Allgemeinen versteht man darunter jede Art von unerwünschter E-Mail.

Spyware

Software, die unentdeckt vom Nutzer private und geheime Anwenderdaten überwacht und über seine Internetverbindung abruft.Dies geschieht in der Regel zu Werbezwecken.Typischerweise werden Spyware-Anwendungen als verborgene Komponenten in Freeware- oder Sharewareprogrammen gebündelt, die aus dem Internet herunter geladen werden können.Es ist jedoch darauf hinzuweisen, dass die Mehrzahl der Shareware- und Freeware-Anwendungen frei von Spyware ist.Ist die Spyware einmal installiert, überwacht sie die Nutzeraktivitäten und überträgt diese Daten im Hintergrund an jemand anderen.Spyware kann auch Informationen über E-Mail-Adressen und sogar Kennwörter und Kreditkartennummern sammeln.

Einem Trojanischen Pferd ähnelt Spyware darin, dass die Anwender das Produkt unwissentlich gemeinsam mit etwas anderem installieren.Eine weit verbreitete Möglichkeit, ein Opfer von Spyware zu werden, ist der Download von bestimmten heute erhältlichen Peer-to-Peer-Dateiaustauschprogrammen (Direktverbindungen von Computern).

Abgesehen von den Fragen der Ethik und des Datenschutzes bestiehlt Spyware den Anwender, indem sie Speicherressourcen seines Rechners nutzt und den Internetzugriff verlangsamt, indem über seine Internetverbindung Informationen an den Spyware-Heimatserver gesendet werden.Da Spyware Speicher und Systemressourcen verbraucht, können die im Hintergrund laufenden Anwendungen zu Systemabstürzen oder allgemeiner Systeminstabilität führen.

Startup Objekt (Autostart-Objekt)

Jede Datei, die sich in diesem Ordner befindet, öffnet sich, wenn der Rechner gestartet wird.Zum Beispiel ein Startbildschirm, eine Sounddatei, die abgespielt wird, wenn der Rechner gestartet wird, ein Erinnerungskalender oder Anwendungsprogramme können Autostart-Objekte sein.Gewöhnlich wird eine Alias-Datei (Verknüpfung) statt der eigentlichen Datei in diesen Ordner gelegt.

Symbolleiste

Die Symbolleiste wurde mit Windows 95 eingeführt und befindet sich auf der Windows Taskleiste (gewöhnlich unten rechts, dort wo sich auch die Uhrzeit befindet).Er enthält kleine Icons zur Information und zum leichteren Zugriff, zum Beispiel: Fax, Drucker, Modem, Lautstärke und mehr.Um auf die Details und Steuerungen zuzugreifen, ist ein Doppelklick oder ein Klick mit der rechten Maustaste erforderlich.

TCP/IP

Transmission Control Protocol/Internet Protocol - Im Internet werden eine Vielzahl von verschiedener Hardware und Betriebssystemen miteinander verbunden.TCP/IP bietet eine Möglichkeit, all diese unterschiedlichen Komponenten zu Kommunikationszwecken miteinander zu verbinden.

Trojaner

Ein vernichtendes Programm, das sich als eine freundliche Anwendung tarnt und auftritt.Im Unterschied zu Viren vervielfältigen sich die Trojaner (auch "trojanische Pferde" genannt) nicht, aber sie können zerstörerisch sein.Einer der heimtückischsten Trojaner ist ein Programm, das behauptet Ihren Rechner von Viren zu befreien, stattdessen aber den Rechner infiziert.Viele Trojaner öffnen den Rechner für den Zugriff von außen.

Der Begriff entstammt einer Geschichte in Homer's "Ilias", in der die Griechen Ihren Feinden, den Trojanern, angeblich als Sühnegabe ein hölzernes Pferd schenkten.Aber, nachdem die Trojaner das Pferd innerhalb der Stadtmauern gebracht hatten, kamen die in dem Bauch des hölzernen Pferdes versteckten Soldaten heraus, öffneten die Tore der Stadt und ermöglichten somit ihren Landsmännern in die Stadt einzudringen und auf diese Weise Troja zu besetzen.

Virus

Ein Programm oder ein Codestück, das auf einen Rechner geladen wird, ohne dass der Benutzer Kenntnis davon hat und welches sich allein ausführt.Die Resultate von Viren können einfache Scherzmeldungen aber auch die Zerstörung von Hardware sein.Die meisten Viren können sich selber vervielfältigen.Alle Computerviren sind von Menschenhand geschrieben.Ein Virus, der sich immer wieder vervielfältigen kann ist sehr einfach zu schreiben.Sogar ein solch einfacher Virus ist fähig, sich durch Netzwerke zu verschicken und Sicherheitssysteme zu überbrücken.

Virusdefinition

Ein binäres Virusmuster, das von einem AntiVirus Programm verwendet wird, um einen Virus zu entdecken und zu entfernen.

Wurm

Ein Programm, das sich über ein Netzwerk verbreitet.Es kann sich nicht an andere Programme anhängen.